Algebraic monodromy groups
of l-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Shiang Tang

Algebraic monodromy groups
of l-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Shiang Tang

In this paper we prove that for any connected reductive algebraic group G and a large enough prime l, there are continuous homomorphisms

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G(\bar{\mathbb{Q}}_l)$$

with Zariski-dense image, in particular we produce the first such examples for $\mathrm{SL}_n, \mathrm{Sp}_{2n}, \mathrm{Spin}_n, E_6^{\mathrm{sc}}$ and E_7^{sc}. To do this, we start with a mod-l representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ related to the Weyl group of G and use a variation of Stefan Patrikis' generalization of a method of Ravi Ramakrishna to deform it to characteristic zero.

1. Introduction

For a split connected reductive group G and a prime number l, it is natural to study two types of continuous representations of $\Gamma_{\mathbb{Q}} = \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$: the mod l representations

$$\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{F}}_l)$$

and the l-adic representations

$$\rho : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$$

where we use the discrete topology for $G(\bar{\mathbb{F}}_l)$ and the l-adic topology for $G(\bar{\mathbb{Q}}_l)$. Mod l representations of $\Gamma_{\mathbb{Q}}$ are closely related to the inverse Galois problem for finite groups of Lie type, which asks for the existence of surjective homomorphisms $\bar{\rho} : \Gamma_{\mathbb{Q}} \twoheadrightarrow G(k)$ for k a finite extension of $\mathbb{F}_l$. It is still wide open, even for small groups such as SL_2. If we replace $\Gamma_{\mathbb{Q}}$ by Γ_F for some number field F, it is not hard to show that every finite group is a Galois group over *some* number field, but if we insist on $\Gamma_{\mathbb{Q}}$ then the problem becomes very difficult. On the other hand, we can ask for its analogs in the l-adic world:

Question 1. Are there continuous homomorphisms $\rho : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$ with Zariski-dense image?

We also ask a refined question which takes geometric Galois representations (in the sense of [Fontaine and Mazur 1995]) into account:

Question 2. Are there continuous geometric Galois representations $\rho : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$ with Zariski-dense image?

This paper gives a complete answer to Question 1. We shall call a reductive group G an l-adic algebraic monodromy group, or simply an l-adic monodromy group for $\Gamma_{\mathbb{Q}}$ if the homomorphisms in Question 1 exist, and a geometric l-adic monodromy group for $\Gamma_{\mathbb{Q}}$ if the homomorphisms in Question 2 exist. We prove the following theorem which gives an almost complete answer to Question 1:

Theorem 1.1 (Main Theorem). *Let G be a connected reductive algebraic group. Then there are continuous homomorphisms*

$$\rho_l : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$$

with Zariski-dense image for large enough primes l.

The key cases of our main theorem are contained the following theorem:

Theorem 1.2. *For a simple algebraic group G, there are infinitely many continuous homomorphisms*

$$\rho_l : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$$

with Zariski-dense image for l large enough. We impose the condition $l \equiv 1(4)$ for $G = B_n^{\mathrm{sc}}, C_n^{\mathrm{sc}}$, and impose $l \equiv 1(3)$ for $G = E_7^{\mathrm{sc}}$.

Remark 1.3. Patrikis has shown that E_7^{ad}, E_8, F_4, G_2 and the L-group of an outer form of E_6^{ad} are geometric l-adic monodromy groups for $\Gamma_{\mathbb{Q}}$, so we will not discuss these cases in the proof of the above theorem. The congruence conditions on l for $G = B_n^{\mathrm{sc}}, C_n^{\mathrm{sc}}, E_7^{\mathrm{sc}}$ can be removed using a theorem proved by Fakhruddin, Khare and Patrikis [2018]. We record it in Theorem 3.21.

It is shown in [Cornut and Ray 2018] that for sufficiently large regular primes p (i.e., a prime p that does not divide the class number of $\mathbb{Q}(\mu_p)$) and for a simple, adjoint group G, there exist a continuous representation of $\Gamma_{\mathbb{Q}}$ into $G(\mathbb{Q}_p)$ with image between the pro-p and the standard Iwahori subgroups of G, which generalizes a theorem of Greenberg [2016] for GL_n. In particular, the image of the Galois group is Zariski-dense. Their construction is nongeometric and is very different from ours. It is unknown whether or not there are infinitely many regular primes, however.

It is an interesting question whether (for instance) SL_n can be a geometric monodromy group for $\Gamma_{\mathbb{Q}}$. The following example shows that Question 2 is more subtle than Question 1, and we should not expect an answer as clean as Theorem 1.1.

Example 1.4. Assuming the Fontaine–Mazur and the Langlands conjectures (see [Fontaine and Mazur 1995; Buzzard and Gee 2014]), there is no homomorphism $\rho : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(\bar{\mathbb{Q}}_l)$ that is unramified almost everywhere, potentially semistable at l, and has Zariski-dense image.

Proof. In fact, by the Fontaine–Mazur and the Langlands conjectures, if such ρ exists, then $\rho = \rho_\pi$ for some cuspidal automorphic representation π on $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$. But ρ is even, i.e., $\det \rho(c) = 1$, π_∞ (the archimedean component of π) is a principal series representation, and π is associated to a Maass form. Therefore, by the Fontaine–Mazur conjecture, ρ_π has finite image, a contradiction. $\square$

In contrast, Theorem 1.2 shows in particular that SL_2 is an l-adic monodromy group for $\Gamma_{\mathbb{Q}}$. On the other hand, SL_2 can be a geometric l-adic monodromy group for Γ_F for *some* finite extension $F/\mathbb{Q}$.

Example 1.5. Let f be a non-CM new eigenform of weight 3, level N, with a nontrivial nebentypus character ε. Such f exist for suitable N, see [LMFDB 2013]. We write E for the field of coefficients of f. Then for all l and $\lambda \mid l$, there is a continuous representation $r_{f,\lambda} : \Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(E_\lambda)$ which is unramified outside $\{v : v \mid Nl\}$ and $\mathrm{Tr}(r_{f,\lambda}(\mathrm{Fr}_p)) = a_p$ for p not dividing Nl, with a_p the p-th Hecke eigenvalue of f. We have $\det(r_{f,\lambda}) = \kappa^2 \varepsilon$ where κ is the l-adic cyclotomic character. By a theorem of Ribet [1985, Theorem 2.1], for almost all l, $\bar{r}_{f,\lambda}(\Gamma_{\mathbb{Q}})$ contains $\mathrm{SL}_2(k)$ for a subfield k of k_λ (the residue field of E_λ). It follows that $r_{f,\lambda}$ has Zariski dense image. If we let F be a finite extension of $\mathbb{Q}$ that trivializes ε, then the image of $r' := \kappa^{-1} \cdot r_{f,\lambda}|_{\Gamma_F}$ lands in $\mathrm{SL}_2(E_\lambda)$ and is Zariski-dense.

The classical groups GSp_n, GSO_n are known as geometric l-adic monodromy groups. Recent work of Arno Kret and Sug Woo Shin [2016] obtains GSpin_{2n+1} as a geometric l-adic monodromy group and Nick Katz [2018] constructs geometric Galois representations with monodromy group GL_n. On the other hand, most of the exceptional algebraic groups are known as geometric l-adic monodromy groups, established in the work of Dettweiler and Reiter [2010], Zhiwei Yun [2014] and Stefan Patrikis [2016]. Patrikis [2016] constructs geometric Galois representations for $\Gamma_{\mathbb{Q}}$ with full algebraic monodromy groups for essentially all exceptional groups of adjoint type. Along the way, Patrikis has obtained an extension to general reductive groups of Ravi Ramakrishna's techniques for lifting odd two-dimensional Galois representations to geometric l-adic representations in [Ramakrishna 2002].

For the rest of this section, we sketch the strategy for proving Theorem 1.2, which makes use of Patrikis' generalization of Ramakrishna's techniques but is very different from his arguments in many ways. For the rest of this section, we assume that G is a simple algebraic group defined over $\mathbb{Z}_l$ with a split maximal torus T. Let $\Phi = \Phi(G, T)$ be the associated root system. Let $\mathcal{O}$ be the ring of integers of an extension of $\mathbb{Q}_l$ whose reduction modulo its maximal ideal is isomorphic to k, a finite extension of $\mathbb{F}_l$. We start with a well-chosen mod l representation and then use a variant of Ramakrishna's method to deform it to characteristic zero with big image. Achieving this is a balancing act between two difficulties: the inverse Galois problem for $G(k)$ is difficult, so we want the residual image to be relatively "small"; on the other hand, Ramakrishna's method works when the residual image is "big".

Let us recall a construction used in [Patrikis 2016]. Patrikis uses the principal GL_2 homomorphism to construct the residual representation

$$\bar{\rho} : \Gamma_{\mathbb{Q}} \xrightarrow{\bar{r}} \mathrm{GL}_2(k) \xrightarrow{\varphi} G(k)$$

for $\bar{r}$ a surjective homomorphism constructed from modular forms and φ a principal GL_2 homomorphism (for its definition, see [Serre 1996; Patrikis 2016, Section 7.1]). But the principal GL_2 is defined only when $\rho^\vee$ (the half-sum of coroots) is in the cocharacter lattice $X_*(T)$, which is not the case for $G = \mathrm{SL}_{2n}$, Sp_{2n}, E_7^{sc}, etc. On the other hand, the principal SL_2 is always defined but it is not known whether $\mathrm{SL}_2(k)$ is a Galois group over $\mathbb{Q}$ and the surjectivity of $\bar{r}$ is crucial in applying Ramakrishna's method.

For this reason, we use a different construction. To simplify notation, we use G, T to denote $G(k)$, $T(k)$, respectively. We consider the following exact sequence of finite groups, which we shall refer to as the N-T sequence:

$$1 \to T \to N_G(T) \xrightarrow{\pi} \mathcal{W} \to 1$$

where $\mathcal{W} = N_G(T)/T$ is the Weyl group of G. We want to take $N = N_G(T)$ as the image of the residual representation $\bar{\rho}$. It turns out that the adjoint action of N on the Lie algebra $\mathfrak{g}$ over k decomposes into at most three irreducible pieces (Corollary 2.2), which is very good for applying Ramakrishna's techniques. It has been known for a long time that $\mathcal{W}$ is a Galois group over $\mathbb{Q}$, but what we need is to realize N as a Galois group over $\mathbb{Q}$. A natural approach would be solving the embedding problem posed by the N-T sequence, i.e., to suppose there is a Galois extension $K/\mathbb{Q}$ realizing $\mathcal{W}$, and then to find a finite Galois extension $K'/\mathbb{Q}$ containing K such that the natural surjective homomorphism $\mathrm{Gal}\,(K'/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}\,(K/\mathbb{Q})$ realizes $\pi : N \twoheadrightarrow \mathcal{W}$.

This embedding problem is solvable when the sequence *splits*, by an elementary case of a famous theorem of Igor Shafarevich, see [Serre 1992, Claim 2.2.5]. In [Adams and He 2017], the splitting of the N-T sequence is determined completely; for instance, it does not split for $G = \mathrm{SL}_n, \mathrm{Sp}_{2n}, \mathrm{Spin}_n, E_7$. We find our way out by replacing N with a suitable subgroup N' for which the decomposition of the adjoint representation remains the same, then realizing N' as a Galois group over $\mathbb{Q}$ with certain properties, see Sections 2A3–2A6. Finally, we define our residual representation $\bar{\rho}$ to be the composite

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N' \to G = G(k)$$

where the first arrow comes from the realization of N' as a Galois group over $\mathbb{Q}$ and the second arrow is the inclusion map. We write $\bar{\rho}(\mathfrak{g})$ for the Lie algebra $\mathfrak{g}/k$ equipped with a $\Gamma_{\mathbb{Q}}$-action induced by the homomorphism

$$\Gamma_{\mathbb{Q}} \xrightarrow{\bar{\rho}} G \xrightarrow{\mathrm{Ad}} \mathrm{GL}(\mathfrak{g}).$$

Now we explain how to deform $\bar{\rho}$ to characteristic zero. This is the hardest part. For a residual representation

$$\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$$

unramified outside a finite set of places S containing the archimedean place and a global deformation condition for $\bar{\rho}$ (which consists of a local deformation condition for each $v \in S$), a typical question in Galois deformation theory is to find continuous l-adic lifts

$$\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$$

of $\bar{\rho}$ such that for all v, $\rho|_{\Gamma_{\mathbb{Q}_v}}$ (we fix an embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_v$) satisfies the prescribed local deformation condition at v. If this can be done, then we can make the image of ρ Zariski-dense in $G(\bar{\mathbb{Q}}_l)$ by specifying a certain type of local deformation condition at a suitable unramified prime.

Ravi Ramakrishna [2002] has an ingenious method for obtaining the desired lifts, which has been generalized and axiomatized in [Taylor 2003; Clozel et al. 2008; Patrikis 2016] and others. By the Poitou–Tate exact sequence, if the dual Selmer group

$$H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g})(1))$$

associated to the global deformation condition for $\bar{\rho}$ vanishes, then such lifts exist. Here $\mathcal{L}$ and $\mathcal{L}^\perp$ are the Selmer system and dual Selmer system of tangent spaces and annihilators of the tangent spaces under the Tate pairing of the given global deformation condition, respectively. Ramakrishna discovered that if one imposes additional local deformation conditions of "Ramakrishna type" in place of the unramified ones at a finite set of well-chosen places of $\mathbb{Q}$ disjoint from S, then the new dual Selmer group will vanish. However, this technique is very sensitive to the image of $\bar{\rho}$, which has to be "big" to make things work; if $\bar{\rho}(\mathfrak{g})$ is irreducible then all is good, but finding such a $\bar{\rho}$ can be very difficult. In practice, we would prefer those $\bar{\rho}$ for which $\bar{\rho}(\mathfrak{g})$ does not decompose too much. Unfortunately, the form of Ramakrishna's method in [Patrikis 2016] (see Theorem 3.4 and its proof for an account of this) does not work for our $\bar{\rho}$.

Inspired by the use of Ramakrishna's method in [Clozel et al. 2008], we surmount this by making two observations. For our $\bar{\rho}$, $\bar{\rho}(\mathfrak{g})$ decomposes into $\bar{\rho}(\mathfrak{t})$ (the Lie algebra of T over k equipped with an irreducible action of $\bar{\rho}(\Gamma_{\mathbb{Q}})$) and a complement (see Corollary 2.2). Our *first observation* is that if

$$H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t}))$$

(see Definition 3.7) vanishes, then we can kill the full dual Selmer group using Ramakrishna's method; moreover, we *cannot* find an auxiliary prime $w \notin S$ at which the Ramakrishna deformation condition (see Definition 3.1) satisfies

$$h^1_{\mathcal{L}^\perp \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{\mathbb{Q},S \cup w}, \bar{\rho}(\mathfrak{g})(1)) < h^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g})(1))$$

when $H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})) \neq \{0\}$. But it is hard to achieve $H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})) = \{0\}$ in general.

Our *second observation* is as follows: suppose that $0 \neq h^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})) \leq h^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})(1))$ (the inequality is easy to guarantee), and let ϕ be a nontrivial class in $H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})(1))$. We can then find an auxiliary prime $w \notin S$ with a Ramakrishna deformation L_w^{Ram} such that $\phi|_{\Gamma_{\mathbb{Q}_w}} \notin L_w^{\mathrm{Ram},\perp}$, which implies

$$h^1_{\mathcal{L}^\perp \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{\mathbb{Q},S \cup w}, \bar{\rho}(\mathfrak{t})(1)) < h^1_{\mathcal{L}^\perp \cup L_{\bar{w}}^{\perp}}(\Gamma_{\mathbb{Q},S \cup w}, \bar{\rho}(\mathfrak{t})(1)),$$

where L_w is the intersection of L_w^{Ram} and the unramified condition at w. It turns out that (see the proof of Proposition 3.13) the right side of the inequality equals $h^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})(1))$; then a double invocation of Wiles' formula gives

$$h^1_{\mathcal{L} \cup L_w^{\mathrm{Ram}}}(\Gamma_{\mathbb{Q},S \cup w}, \bar{\rho}(\mathfrak{t})) < h^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t})).$$

By induction, we can enlarge $\mathcal{L}$ finitely many times to make $H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{t}))$ vanish, which in turn allows us (see the proof of Theorem 3.16) to enlarge $\mathcal{L}$ even further to make $H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g})(1))$ vanish, as

remarked in the first observation. Thus we obtain an l-adic lift $\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$ satisfying the prescribed local deformation conditions.

The above variation of Ramakrishna's method is devised very specifically for the residual representation we construct. We do not know how to generalize these ideas to the case of an arbitrary residual representation.

Remark 1.6. For technical reasons, our method does not work for SL_2, SL_3, $Spin_7$; see Proposition 2.9 and Remark 2.14. Nevertheless, an easy variant of Ramakrishna's original method applies to SL_2, Patrikis' extension of Ramakrishna's method applies to SL_3 and $Spin_7$. Patrikis' method also applies to E_6^{sc} with minor modifications, and we use it in this paper. Our method should work for E_6^{sc} as well, modulo an instance of the inverse Galois theory, but we do not pursue it here.

Notation. For a field F (typically $\mathbb{Q}$ or $\mathbb{Q}_p$), we let Γ_F denote $Gal\,(\overline{F}/F)$ for some fixed choice of algebraic closure of $\overline{F}$ of F. When F is a number field, for each place v of F we fix once and for all embeddings $\overline{F} \to \overline{F}_v$, giving rise to inclusions $\Gamma_{F_v} \to \Gamma_F$. If S is a finite set of places of F. we let $\Gamma_{F,S}$ denote $Gal\,(F_S/F)$, where F_S is the maximal extension of F in $\overline{F}$ unramified outside of S. If v is a place of F outside S, we write Fr_v for the corresponding arithmetic frobenius element in $\Gamma_{F,S}$. When $F = \mathbb{Q}$, we will sometimes write Γ_v for Γ_{F_v} and Γ_S for $\Gamma_{\mathbb{Q},S}$. For a representation ρ of Γ_F, we let $F(\rho)$ denote the fixed field of $Ker(\rho)$.

Consider a group Γ, a ring A, an algebraic group G over $Spec(A)$, and a homomorphism $\rho : \Gamma \to G(A)$. We write $\mathfrak{g}$ for both the Lie algebra of G and the $A[G]$-module induced by the adjoint action. We let $\rho(\mathfrak{g})$ denote the $A[\Gamma]$-module with underlying A-module $\mathfrak{g}$ induced by ρ. Similarly, for a $A[G]$-submodule M of $\mathfrak{g}$, we write $\rho(M)$ for the $A[\Gamma]$-module with underlying A-module M induced by ρ.

We call an algebraic group *simple* if it is connected, nonabelian and has no proper normal algebraic subgroups except for finite subgroups. It is sometimes called an almost simple group in the literature. Consider a simple algebraic group G, we write G^{sc} and G^{ad} for the simply connected form and adjoint form of G, respectively.

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_l$. We let $CNL_{\mathcal{O}}$ denote the category of complete noetherian local $\mathcal{O}$-algebras for which the structure map $\mathcal{O} \to R$ induces an isomorphism on residue fields.

All the Galois cohomology groups we consider will be k-vector spaces for k a finite extension of $\mathbb{F}_l$. We abbreviate $\dim H^n(-)$ by $h^n(-)$.

We write κ for the l-adic cyclotomic character, and $\bar{\kappa}$ for its mod l reduction.

2. Constructions of residual representations

In this section, we construct residual representations

$$\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(\overline{\mathbb{F}}_l)$$

for G a simple, *simply connected* algebraic group.

2A. *Constructions based on the Weyl groups.* Let k be a finite extension of $\mathbb{F}_l$. We consider the group of k-points of the normalizer of a split maximal torus of G and hope to realize it as the Galois group of some extension of $\mathbb{Q}$.

2A1. *Some group-theoretic results.* We recall a property of the Weyl group of an *irreducible* root system Φ.

Lemma 2.1. *The Weyl group $\mathcal{W}$ acts irreducibly on the $\mathbb{C}$-vector space spanned by Φ and transitively on roots of the same length.*

Let $G = G(k)$ and $T = T(k)$, a maximal split torus of G. Let $\Phi = \Phi(G, T)$ and $N = N_G(T)$.

Corollary 2.2. *For any $\alpha, \beta \in \Phi$ of the same length, there exists $w \in N$ such that $\mathrm{Ad}(w)\mathfrak{g}_\alpha = \mathfrak{g}_\beta$. The adjoint action $\mathrm{Ad}(N)$ on $\mathfrak{g}$ decomposes into submodules $\mathfrak{t}$ and*

$$\mathfrak{g}_\Phi := \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

when Φ is simply laced, and is the direct sum of $\mathfrak{t}$,

$$\mathfrak{g}_l := \sum_{\alpha \in \Phi,\, \alpha \text{ is long}} \mathfrak{g}_\alpha,$$

and

$$\mathfrak{g}_s := \sum_{\alpha \in \Phi,\, \alpha \text{ is short}} \mathfrak{g}_\alpha$$

otherwise.

Moreover, as an N-module, $\mathfrak{t}$ is irreducible, and $\mathfrak{g}_\Phi$, $\mathfrak{g}_l$, $\mathfrak{g}_s$ are irreducible if l is sufficiently large.

Proof. It suffices to show that $\mathfrak{g}_\Phi$, $\mathfrak{g}_l$, $\mathfrak{g}_s$ are irreducible N-modules. We will only show that $\mathfrak{g}_\Phi$ is irreducible, for the other two cases are similar. Take a nonzero vector $X \in \mathfrak{g}_\Phi$, write $X = \sum_{1 \le i \le k} X_i$ where $0 \ne X_i \in \mathfrak{g}_{\alpha_i}$ for some distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_k \in \Phi$. Since l is sufficiently large, we can choose $t \in T$ such that $\alpha(t)$, $\alpha \in \Phi$ are all distinct. We have

$$\mathrm{ad}(t^j)X = \sum_i \alpha_i(t)^j X_i$$

where $0 \le j \le k - 1$. As the X_i's are linearly independent and the determinant of the coefficient matrix is nonzero,

$$X, \mathrm{ad}(t)X, \mathrm{ad}(t^2)X, \ldots, \mathrm{ad}(t^{k-1})X$$

are linearly independent and hence they span the same subspace as $X_1, \ldots, X_k$ do. In particular, $X_i \in \mathfrak{g}_{\alpha_i}$ belongs to the N-submodule of $\mathfrak{g}_\Phi$ generated by X. Because N acts transitively on the set of root spaces, it follows that X generates $\mathfrak{g}_\Phi$. Therefore, $\mathfrak{g}_\Phi$ is irreducible. $\qquad\square$

Remark 2.3. Corollary 2.2 remains valid for a subgroup N' of N that maps onto a subgroup W' of W acting transitively on roots of the same length.

2A2. *Some results in the inverse Galois theory.* We record some elementary results (with proofs) about inverse Galois theory, some of which are modified in order to satisfy our purposes. See Serre's lecture notes [1992] for details.

Theorem 2.4. *For $n \geq 2$, there are infinitely many polynomials with $\mathbb{Q}$-coefficients that realize the symmetric group of n letters S_n (or the alternating group of n letters A_n) as a Galois group over $\mathbb{Q}$. Moreover, for S_n (or for A_n with $n \geq 4$), the polynomial can be chosen to have at least a pair of nonreal roots.*

Proof. See [Serre 1992, Sections 4.4 and 4.5]. For the last part, we consider the polynomial $f(X, T)$ on page 42 of [loc. cit.]. For any rational value of T, it has at most three real roots by inspection, so it must have at least a nonreal root when $n \geq 4$. For $n = 2, 3$, it is easy to find such polynomials. The demonstration for A_n is similar, see the polynomial $h(X, T)$ on page 44. $\square$

The next result is an elementary case of a theorem of Igor Shafarevich, which will be used frequently in our constructions:

Theorem 2.5. *Let G be a finite group. Suppose that there is a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. Let H be a finite abelian group with exponent m. Suppose that there is a* split *exact sequence of finite groups*

$$1 \to H \to S \to G \to 1.$$

Then there is a finite Galois extension $M/\mathbb{Q}$ containing K such that the natural surjective homomorphism $\mathrm{Gal}(M/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$ realizes the surjective homomorphism $S \twoheadrightarrow G$. In other words, a split embedding problem with abelian kernel always has a proper solution.

Moreover, for any prime l that is outside the ramification locus of $K/\mathbb{Q}$ and prime to m, we can choose M so that l is unramified in M.

Proof. The argument is a minor modification of the proof of [Serre 1992, Claim 2.2.5]. Put $L = K(\mu_m)$. H can be regarded as a m-torsion module on which $\mathrm{Gal}(L/\mathbb{Q})$ acts. So there is a finite free $(\mathbb{Z}/m\mathbb{Z})[\mathrm{Gal}(L/\mathbb{Q})]$-module F of which H is a quotient. Suppose that r is the number of copies of $(\mathbb{Z}/m\mathbb{Z})[\mathrm{Gal}(L/\mathbb{Q})]$ in F. Let S' be the semidirect product of $\mathrm{Gal}(L/\mathbb{Q})$ and F. To solve the embedding problem posed by $1 \to H \to S \to G \to 1$, it suffices to solve the embedding problem posed by

$$1 \to F \to S' \to \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

Claim. There is a Galois extension $M'/\mathbb{Q}$ that solves the above embedding problem. Moreover, for any prime l that does not divide m and is outside the ramification locus of $K/\mathbb{Q}$, we can choose M' so that l is unramified in M'.

To see this, we choose places $v_1, \ldots, v_r$ of $\mathbb{Q}$ away from l such that v_i *splits completely* in L. Let w_i be a place of L extending v_i, $1 \leq i \leq r$. Any place of L extending v_i can be written *uniquely* as σw_i for some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Let w_0 be a place of L extending l. For $1 \leq i \leq r$, choose $\theta_i \in \mathcal{O}_L$ such that for

$0 \le j \le r$, $(\sigma w_j)(\theta_i) = 1$ if $\sigma = 1$ and $i = j$ and 0 if not. The existence of θ_i follows from the weak approximation theorem. Let

$$M' = L(\sqrt[m]{\sigma \theta_i} \mid \sigma \in \mathrm{Gal}\,(L/\mathbb{Q}), 1 \le i \le r),$$

which is Galois over $\mathbb{Q}$, being the composite of L and the splitting field of the polynomial

$$\prod_i \prod_\sigma (T^m - \sigma \theta_i) \in \mathbb{Q}[T].$$

It is easy to see that $\mathrm{Gal}\,(M'/L)$ is isomorphic to F as $\mathrm{Gal}\,(L/\mathbb{Q})$-modules. In fact, for each i there is an isomorphism

$$\phi_i : \mathrm{Gal}(L(\sqrt[m]{\sigma \theta_i} \mid \sigma \in \mathrm{Gal}\,(L/\mathbb{Q}))/L) \cong (\mathbb{Z}/m\mathbb{Z})[\mathrm{Gal}(L/\mathbb{Q})].$$

For an element g on the left side and any $\sigma \in \mathrm{Gal}\,(L/\mathbb{Q})$, $g(\sqrt[m]{\sigma \theta_i}) = \zeta_\sigma \cdot \sqrt[m]{\sigma \theta_i}$ for some $\zeta_\sigma \in \mu_m \cong \mathbb{Z}/m\mathbb{Z}$. We then define

$$\phi_i(g) = \sum_\sigma \zeta_\sigma \cdot \sigma \in (\mathbb{Z}/m\mathbb{Z})[\mathrm{Gal}\,(L/\mathbb{Q})].$$

It is clear that ϕ_i is an isomorphism by our choice of θ_i. It follows that $\mathrm{Gal}\,(M'/L) \cong F$ by linear disjointness.

Therefore, we obtain an exact sequence

$$1 \to F \to \mathrm{Gal}(M'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

Since $F \cong \mathrm{Ind}_{\{1\}}^{\mathrm{Gal}\,(L/\mathbb{Q})} \mathbb{Z}/m\mathbb{Z}$, by Shapiro's lemma, $H^2(\mathrm{Gal}\,(L/\mathbb{Q}), F) = H^2(\{1\}, \mathbb{Z}/m\mathbb{Z}) = \{0\}$, hence the sequence splits. Thus, $\mathrm{Gal}(M'/\mathbb{Q}) \cong S'$.

It remains to show that l is unramified in M'. For any σ in $\mathrm{Gal}\,(L/\mathbb{Q})$ and for any i, w_0 is unramified in $L(\sqrt[m]{\sigma \theta_i})$, because $w_0(\sigma \theta_i) = 0$ and l does not divide m. So w_0 is unramified in their composite M'. On the other hand, l is unramified in K by assumption and is unramified in $\mathbb{Q}(\mu_m)$ since l does not divide m, so l is unramified in L. It follows that l is unramified in M', proves the claim.

Finally, letting M be the fixed field of the kernel of the natural surjective homomorphism $S' \twoheadrightarrow S$, we obtain a solution to the original embedding problem. $\square$

2A3. SL_n. Let $G = \mathrm{SL}_n(k)$, so $\mathcal{W} \cong S_n$. By [Adams and He 2017], the N-T sequence splits only when n is odd. We consider the subgroup $\mathcal{W}' = A_n$ of $\mathcal{W}$. Let T be the maximal torus of diagonal elements in $\mathrm{SL}_n(k)$ and let Φ be $\Phi(G, T)$.

Lemma 2.6. *Suppose $n \ge 4$. Then A_n, as a subgroup of $\mathcal{W}$, acts transitively on Φ.*

Proof. This follows from the fact that A_n acts doubly transitively on $\{1, 2, \ldots, n\}$ if and only if $n \ge 4$. $\square$

Let $N' = \pi^{-1}(\mathcal{W}')$, where π is the natural map from $N_G(T)$ to $\mathcal{W}$.

Lemma 2.7. *The following exact sequence of finite groups splits*:

$$1 \to T \to N' \to \mathcal{W}' \to 1.$$

Proof. We think of A_n as a subgroup of $N = N_G(T)$ by realizing it as the group of $n \times n$ *even* permutation matrices. Then A_n normalizes T and N' is a semidirect product of them. $\square$

Let l be large enough. Since T is abelian of exponent $|k| - 1$ which is prime to l, by Theorems 2.4 and 2.5, there is a surjection $\Gamma_{\mathbb{Q}} \twoheadrightarrow N'$ which is unramified at l. Moreover, by choosing a rational polynomial with nonreal roots that realizes A_n as a Galois group over $\mathbb{Q}$, we can make the complex conjugation map to an element away from the center of G. Define $\bar{\rho}$ to be the composite

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N' \xrightarrow{\ i\ } \mathrm{SL}_n(k).$$

Remark 2.8. It is trickier to realize N as a Galois group over $\mathbb{Q}$. This can be reduced to realizing the "Tits group" $\mathcal{T}$ of SL_n as a Galois group. $\mathcal{T}$ can be identified with the group of $n \times n$ signed permutation matrices with determinant one, which is an index two subgroup of the group of $n \times n$ signed permutation matrices. The latter is isomorphic to the Weyl group of type B_n, hence known to be a Galois group over $\mathbb{Q}$. As the N-T sequence splits if and only if n is odd, by Theorem 2.5, $\mathcal{T}$ can be realized over $\mathbb{Q}$ for n odd. When n is even, this problem is open except for small n, as far as the author knows.

Let $\mathfrak{g} = \mathfrak{sl}_n(k)$.

Proposition 2.9. *For l sufficiently large and $n \geq 4$, $\bar{\rho}(\mathfrak{g})$ decomposes into irreducible $\Gamma_{\mathbb{Q}}$-modules $\bar{\rho}(\mathfrak{t})$ and $\bar{\rho}(\mathfrak{g}_{\Phi})$.*

Proof. This follows from Corollary 2.2 and Remark 2.3. $\square$

There remains the case when G is SL_2 or SL_3. For SL_3, see Section 2B. For SL_2, see Section 4B3.

2A4. Sp_{2n}. Let $G = \mathrm{Sp}_{2n}(k)$, then $\mathcal{W}$ is isomorphic to a semidirect product of S_n and $D := (\mathbb{Z}/2\mathbb{Z})^n$. We fix a maximal split torus T in $\mathrm{Sp}_{2n}(k)$. The N-T sequence does not split by [Adams and He 2017].

Lemma 2.10. *Consider the N-T sequence for Sp_{2n}. The group $S_n \subset \mathcal{W}$ has a section to N, whereas $D \subset \mathcal{W}$ does not have a section to N but there is a subgroup $\tilde{D}$ of N such that $\pi(\tilde{D}) = D$ and $\tilde{D} \cong (\mathbb{Z}/4\mathbb{Z})^n$. Moreover, as subgroups of N, S_n normalizes $\tilde{D}$ and $S_n \cap \tilde{D} = \{1\}$.*

We let $\mathcal{W}_1$ be the subgroup of N generated by S_n and $\tilde{D}$.

Proof. Let $V = k^{2n}$ be the $2n$-dimensional vector space over k endowed with a nondegenerate alternating form $(\cdot, \cdot)$. We may choose a basis

$$e_1, \ldots, e_n, e'_1, \ldots, e'_n$$

of V such that $(e_i, e'_j) = 1$ if and only if $i = j$, and that $(e_i, e_j) = 0$, $(e'_i, e'_j) = 0$ for all i, j. The Weyl group of Sp_{2n} is isomorphic to the semidirect product of the group S_n, which acts by permuting $e_1, \ldots, e_n$, and the group $D := (\mathbb{Z}/2\mathbb{Z})^n$, which acts by $e_i \mapsto (\pm 1)_i e_i$. There is an inclusion $S_n \to \mathrm{Sp}_{2n}(k)$ (which is a section to $N \to \mathcal{W}$) given as follows: $\forall \sigma \in S_n$, σ permutes $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n$ by permuting the indices, which defines an element in $\mathrm{Sp}_{2n}(k)$. There is no such inclusion for D. However, we can define a 2-group $\tilde{D}$ which embeds into $\mathrm{Sp}_{2n}(k)$ as follows: for $1 \leq i \leq n$, let d_i be an endomorphism of V such that $d_i(e_i) = -e'_i$, $d_i(e'_i) = e_i$, and d_i fixes all other basis vectors. It is clear that $d_i \in \mathrm{Sp}_{2n}(k)$. Let

$\tilde{D}$ be the subgroup of $\mathrm{Sp}_{2n}(k)$ generated by d_i for $1 \leq i \leq n$. Then $\tilde{D} \cong (\mathbb{Z}/4\mathbb{Z})^n$. It is obvious that (as subgroups of $\mathrm{Sp}_{2n}(k)$) S_n normalizes $\tilde{D}$ and $S_n \cap \tilde{D} = \{1\}$. $\qquad\square$

Therefore, by Theorem 2.4 and 2.5, $\mathcal{W}_1$ can be realized as a Galois group over $\mathbb{Q}$ such that the complex conjugation corresponds to an element away from the center of G. The group N is generated by $\mathcal{W}_1$ and T. We have $\mathcal{W}_1$ normalizes T and $\mathcal{W}_1 \cap T \cong (\mathbb{Z}/2\mathbb{Z})^n$. Let S be the (abstract) semidirect product of $\mathcal{W}_1$ and T. By Theorem 2.5, for l large enough, S can be realized as a Galois group over $\mathbb{Q}$ unramified at l. Composing the corresponding map $\Gamma_{\mathbb{Q}} \twoheadrightarrow S$ with the natural surjection $S \twoheadrightarrow N$, we obtain a surjection $\Gamma_{\mathbb{Q}} \twoheadrightarrow N$ that is unramified at l and for which the complex conjugation maps to an element outside the center of G. Define $\bar{\rho}$ to be the composite

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N \xrightarrow{i} \mathrm{Sp}_{2n}(k).$$

Let $\mathfrak{g} = \mathfrak{sp}_{2n}(k)$. The root system Φ of $\mathfrak{g}$ is not simply laced.

Proposition 2.11. *For l sufficiently large, $\bar{\rho}(\mathfrak{g})$ decomposes into irreducible $\Gamma_{\mathbb{Q}}$-modules $\bar{\rho}(\mathfrak{t})$, $\bar{\rho}(\mathfrak{g}_l)$ and $\bar{\rho}(\mathfrak{g}_s)$.*

Proof. This follows from Corollary 2.2. $\qquad\square$

2A5. *Spin_{2n} and Spin_{2n+1}.* For spin groups, the N-T sequence does not split by [Adams and He 2017]. For $G = \mathrm{Spin}_{2n}$, $\mathcal{W}$ is isomorphic to a semidirect product of S_n and $D := (\mathbb{Z}/2\mathbb{Z})^{n-1}$ and we let $\mathcal{W}'$ be the subgroup generated by A_n and D. For $G = \mathrm{Spin}_{2n+1}$, $\mathcal{W}$ is isomorphic to a semidirect product of S_n and $D := (\mathbb{Z}/2\mathbb{Z})^n$ and we let $\mathcal{W}'$ be the subgroup generated by A_n and D. Similar to the symplectic case, we will show that $N' = \pi^{-1}(\mathcal{W}')$ is a Galois group over $\mathbb{Q}$.

Lemma 2.12. *Consider the N-T sequence for $G = \mathrm{Spin}_{2n}(k)$ or $\mathrm{Spin}_{2n+1}(k)$. The map $\pi^{-1}(A_n) \to A_n$ admits a section, and there is a nilpotent subgroup $\tilde{D}$ of N such that $\pi(\tilde{D}) = D$. Moreover, as subgroups of N, A_n normalizes $\tilde{D}$ and we let $\mathcal{W}_1$ be their product.*

Proof. Let $\underline{G} := \mathrm{SO}_{2n}(k)$ or $\mathrm{SO}_{2n+1}(k)$. We have the standard homomorphism $i : \mathrm{GL}_n(k) \to \underline{G}$, which restricts to a homomorphism $S_n \to \underline{G}$. Let $\widetilde{\mathrm{GL}}_n(k)$ be the pullback of i along the covering map $G \to \underline{G}$. It is a two-fold central extension of $\mathrm{GL}_n(k)$, which can be identified with the group of pairs (g, z) with $g \in \mathrm{GL}_n(k)$, $z \in k^{\times}$, such that $\det g = z^2$, where the multiplication is defined by $(g_1, z_1) \cdot (g_2, z_2) = (g_1 g_2, z_1 z_2)$. A subgroup H of $\mathrm{GL}_n(k)$ has a section in $\widetilde{\mathrm{GL}}_n(k)$ if and only if the restriction of $\det$ to H is the square of a character of H. In particular, taking $H = A_n$, we see that A_n has a section to $\widetilde{\mathrm{GL}}_n(k)$. It follows that $\pi^{-1}(A_n) \to A_n$ admits a section.

The map $\underline{\pi}^{-1}(D) \to D$ has a section, where $\underline{\pi}$ is the natural map $N_{\underline{G}}(\underline{T}) \to \mathcal{W}$; this follows from [Adams and He 2017, Theorem 4.16], or can be seen directly from an elementary matrix calculation. Let $\tilde{D} \subset G$ be the preimage of $D \subset \underline{G}$ under the covering map $G \to \underline{G}$. As D is abelian, $[\tilde{D}, \tilde{D}] = Z(G) \cong \mu_2$. In particular, $\tilde{D}$ is nilpotent.

Finally, because A_n normalizes D in $\underline{G}$, A_n normalizes $\tilde{D}$ in G. $\qquad\square$

Therefore, by Theorem 2.4 and Shafarevich's theorem (the group $\tilde{D}$ is nilpotent, see [Neukirch et al. 2000, IX, Section 6] for Shafarevich's theorem), $\mathcal{W}_1$ can be realized as a Galois group over $\mathbb{Q}$ such that the complex conjugation corresponds to an element outside the center of G. Let N' be the subgroup of G generated by $\mathcal{W}_1$ and T ($\mathcal{W}_1$ normalizes T). Let S be the (abstract) semidirect product of $\mathcal{W}_1$ and T. By Theorem 2.5, for l large enough, S can be realized as a Galois group over $\mathbb{Q}$ unramified at l. Composing the corresponding map $\Gamma_{\mathbb{Q}} \twoheadrightarrow S$ with the natural quotient map $S \twoheadrightarrow N'$, we obtain a surjection

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N'$$

that is unramified at l and for which the complex conjugation maps to an element outside the center of G (since the complex conjugation corresponds to an element outside the center of G in the realization of $\mathcal{W}_1$ as a Galois group over $\mathbb{Q}$). For $G = \mathrm{Spin}_{2n}$ or Spin_{2n+1}, define $\bar{\rho}$ to be the composite

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N' \xrightarrow{\;i\;} G(k).$$

Let $\mathfrak{g}$ be the Lie algebra of $G(k)$. The corresponding root system Φ is simply laced if $G = \mathrm{Spin}_{2n}$ and is not if $G = \mathrm{Spin}_{2n+1}$.

Proposition 2.13. *For l sufficiently large and $n \geq 4$, $\bar{\rho}(\mathfrak{g})$ decomposes into irreducible $\Gamma_{\mathbb{Q}}$-modules $\bar{\rho}(\mathfrak{t})$ and $\bar{\rho}(\mathfrak{g}_\Phi)$ when $G = \mathrm{Spin}_{2n}$; and it decomposes into irreducible $\Gamma_{\mathbb{Q}}$-modules $\bar{\rho}(\mathfrak{t})$, $\bar{\rho}(\mathfrak{g}_l)$ and $\bar{\rho}(\mathfrak{g}_s)$ when $G = \mathrm{Spin}_{2n+1}$.*

Proof. Note that the action of $\mathcal{W}'$ on Φ is transitive if and only if $n \geq 4$. Then the proposition follows from Corollary 2.2 and Remark 2.3. $\qquad\square$

Remark 2.14. There remains the case when G is one of Spin_4, Spin_5, Spin_6, Spin_7. But $\mathrm{Spin}_4(\bar{\mathbb{Q}}_l) \cong \mathrm{SL}_2(\bar{\mathbb{Q}}_l) \times \mathrm{SL}_2(\bar{\mathbb{Q}}_l)$, $\mathrm{Spin}_5(\bar{\mathbb{Q}}_l) \cong \mathrm{Sp}_4(\bar{\mathbb{Q}}_l)$, $\mathrm{Spin}_6(\bar{\mathbb{Q}}_l) \cong \mathrm{SL}_4(\bar{\mathbb{Q}}_l)$ which are included in other cases. For Spin_7, the half sum of coroots $\rho^\vee = 3\alpha_1^\vee + 5\alpha_2^\vee + 3\alpha_3^\vee$ has integer coefficients, so the principal GL_2 map is well defined, see Section 2B.

2A6. E_7^{sc}. Let $G = E_7^{\mathrm{sc}}(k)$. The Weyl group $\mathcal{W}$ is isomorphic to the direct product of $[\mathcal{W}, \mathcal{W}]$ and $\mathbb{Z}/2\mathbb{Z}$. By [Adams and He 2017], the N-T sequence does not split. We choose a subgroup $\mathcal{W}'$ of $\mathcal{W}$ which lifts to N as follows. Consider the extended Dynkin diagram of type E_7, there is a subroot system Φ' of Φ which is of type A_7. The alternating group A_8 is a subgroup of $S_8 \cong \mathcal{W}(A_7) \leq \mathcal{W} = \mathcal{W}(E_7)$.

Lemma 2.15. *The group $A_8 \leq \mathcal{W}$ lifts to N.*

Proof. This is because A_8 lifts to SL_8. $\qquad\square$

Lemma 2.16. *The action of A_8 on Φ has an orbit of size 56 and an orbit of size 70.*

Proof. We first consider the action of $S_8 \cong \mathcal{W}(A_7)$ on Φ. By Lemma 2.1, S_8 acts transitively on Φ', which has 56 roots. A straightforward calculation using Plate E_7 in [Bourbaki 1968] shows that for some $\alpha \in \Phi - \Phi'$, $S_8 \cdot \alpha$ has exactly 70 roots (in the extended Dynkin diagram, take α to be the simple root that is not in Φ', then we let the group generated by the simple reflections in Φ' act on α and count the number of roots in the orbit). So the stabilizer of α in S_8 is isomorphic to $S_4 \times S_4 \subset S_8$. Since

$56 + 70 = 126$ is the number of roots in Φ, the lemma is true for S_8. Now we consider the alternating group A_8. Lemma 2.6 implies that A_8 still acts transitively on Φ'. As $(S_4 \times S_4) \cap A_8$ (the stabilizer of α in A_8) has order $\frac{1}{2}|S_4 \times S_4| = 288$, the orbit $A_8 \cdot \alpha$ has exactly $|A_8|/288 = 70$ roots. $\qquad\square$

It is clear that A_8, considered as a subgroup of N, normalizes T and $A_8 \cap T = \{1\}$. Let N' be the subgroup of $G = E_7^{\mathrm{sc}}(k)$ generated by A_8 and T. By Theorems 2.4 and 2.5, for l large enough, we can find a continuous surjection

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N'$$

that is unramified at l and for which the complex conjugation maps to an element away from the center of G. Define $\bar{\rho}$ to be the composite

$$\Gamma_{\mathbb{Q}} \twoheadrightarrow N' \xrightarrow{\ i\ } E_7^{\mathrm{sc}}(k).$$

Let $\mathfrak{g}_a$ and $\mathfrak{g}_b$ be the direct sums of the root spaces corresponding to the orbit of size 56 and size 70, respectively, in Lemma 2.16.

Proposition 2.17. *For l sufficiently large, $\bar{\rho}(\mathfrak{g})$ decomposes into irreducible $\Gamma_{\mathbb{Q}}$-modules $\bar{\rho}(\mathfrak{t})$, $\bar{\rho}(\mathfrak{g}_a)$ and $\bar{\rho}(\mathfrak{g}_b)$.*

Proof. The proof is very similar to the proof of Corollary 2.2. $\qquad\square$

2B. *The principal GL_2 construction.* We record some facts on the principal SL_2 and GL_2. For more details, see [Serre 1996, Section 1]. Let G/k be a simple algebraic group with a Borel B containing a split maximal torus T with unipotent radical U. Let $\Phi = \Phi(G, T)$ be the root system of G with the set of simple roots Δ corresponding to B. We fix a pinning $\{x_\alpha : \mathbb{G}_a \to U_\alpha\}$ where U_α is the root subgroup in B corresponding to α. Let $X_\alpha = dx_\alpha(1)$ for all $\alpha \in \Delta$ and let

$$X = \sum_{\alpha \in \Delta} X_\alpha,$$

which can be extended to an $\mathfrak{sl}_2$-triple (X, H, Y) where

$$H = \sum_{\alpha > 0} H_\alpha$$

with H_α the coroot vector corresponding to α.

When p is large enough relative to G, there is an exponential map

$$\exp : \mathrm{Lie}(U) \to U$$

which is an isomorphism.

A *principal SL_2 homomorphism* is a homomorphism

$$\varphi : \mathrm{SL}_2 \to G$$

such that

$$\varphi\left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\right) = \exp(tX), \quad \varphi\left(\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}\right) = 2\rho^\vee(t)$$

where $\rho^\vee$ is the half-sum of the coroots. $\rho^\vee$ is always defined when G is adjoint. Suppose that $\rho^\vee : \mathbb{G}_m \to G^{\mathrm{ad}}$ lifts to G and we fix a lift which is again denoted $\rho^\vee$. A *principal* GL_2 *homomorphism* is a homomorphism

$$\varphi : \mathrm{GL}_2 \to G$$

that extends a principal SL_2 such that such that

$$\varphi\left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\right) = \exp(tX), \quad \varphi\left(\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}\right) = \rho^\vee(t).$$

By definition, a principal GL_2 factors through PGL_2.

By examining the list in [Bourbaki 1968], we get:

Lemma 2.18. *For G a simple algebraic group, $\rho^\vee : \mathbb{G}_m \to G^{\mathrm{ad}}$ lifts to G^{sc} if and only if G is one of the following types*: A_{2n}, B_{4n}, B_{4n+3}, D_{4n}, D_{4n+1}, E_6, E_8, F_4, G_2.

The operator $\mathrm{ad}(H)$ preserves $\mathfrak{g}^X$ (the centralizer of X in $\mathfrak{g}$) and

$$\mathfrak{g}^X = \sum_{m>0} V_{2m},$$

where V_{2m} is the eigenspace of H corresponding to the eigenvalue $2m$. The following proposition is due to Kostant [1959].

Proposition 2.19. *The dimension of $\mathfrak{g}^X$ is equal to the rank of $\mathfrak{g}$. V_{2m} is nonzero if and only if m is an exponent of $\mathfrak{g}$. Letting GL_2 act on $\mathfrak{g}$ via φ, there is an isomorphism of GL_2-representations*

$$\mathfrak{g} \cong \bigoplus_{m>0} \mathrm{Sym}^{2m}(k^2) \otimes \det^{-m} \otimes V_{2m}.$$

Suppose that $\rho^\vee : \mathbb{G}_m \to G^{\mathrm{ad}}$ lifts to G. We take f to be as in Example 1.5. By [Ribet 1985, Theorem 2.1], the projective image of $\bar{r}_{f,\lambda}$ is either $\mathrm{PGL}_2(k)$ or $\mathrm{PSL}_2(k)$ for a subfield k of k_λ. We then define

$$\bar{\rho} : \Gamma_{\mathbb{Q}} \xrightarrow{\bar{r}_{f,\lambda}} \mathrm{GL}_2(k) \xrightarrow{\varphi} G(k).$$

This construction works for all exceptional groups but E_7^{sc} as $\rho^\vee : \mathbb{G}_m \to E_7^{\mathrm{ad}}$ does not lift to E_7^{sc}. We will only use this construction for G of type E_6, A_2 and B_3.

3. Ramakrishna's method and its variants

Given $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ defined in the previous section, we want to obtain an l-adic lift $\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$ with $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_l$ whose residue field is k satisfying a given global deformation condition. Just as in [Patrikis 2016], we use Ramakrishna's method to annihilate the associated

dual Selmer group. The new feature is a double use of Patrikis' extension of Ramakrishna's method when the original form fails to work, see Section 3B.

3A. *Ramakrishna's method.*

3A1. *Ramakrishna deformations.* We list the key points and results of Patrikis' extension of Ramakrishna's method. For proofs, see [Patrikis 2016, Section 4.2]. For an overview on the deformation theory of (G-valued) Galois representations, see [loc. cit., Section 3].

We begin by defining a type of local deformation condition called Ramakrishna's condition, which will be imposed at the auxiliary primes of ramification in Ramakrishna's global argument. Let F be a finite extension of $\mathbb{Q}_p$ for $p \neq l$, and let $\bar{\rho} : \Gamma_F \to G(k)$ be an *unramified* homomorphism such that $\bar{\rho}(\mathrm{Fr}_F)$ is a regular semisimple element. Let T be the connected component of the centralizer of $\bar{\rho}(\mathrm{Fr}_F)$; this is a maximal k-torus of G, but we can lift it to an $\mathcal{O}$-torus uniquely up to isomorphism, which we also denote by T, and then we can lift the embedding over k to an embedding over $\mathcal{O}$ which is unique up to $\hat{G}(\mathcal{O})$-conjugation. By passing to an étale extension of $\mathcal{O}$, we may assume that T is split.

The following definition is from [loc. cit.].

Definition 3.1. Let $\bar{\rho}, T$ be as above. For $\alpha \in \Phi(G, T)$, $\bar{\rho}$ is said to be of Ramakrishna type α if

$$\alpha(\bar{\rho}(\mathrm{Fr}_F)) = \bar{\kappa}(\mathrm{Fr}_F).$$

Let $H_\alpha = T \cdot U_\alpha$ be the subgroup generated by T and the root subgroup U_α corresponding to α. Ramakrishna deformation is a functor

$$\mathrm{Lift}_{\bar{\rho}}^{\mathrm{Ram}} : \mathrm{CNL}_{\mathcal{O}} \to \mathbf{Sets}$$

such that for a complete local noetherian $\mathcal{O}$-algebra R, $\mathrm{Lift}_{\bar{\rho}}^{\mathrm{Ram}}(R)$ consists of all lifts

$$\rho : \Gamma_F \to G(R)$$

of $\bar{\rho}$ such that ρ is $\hat{G}(R)$-conjugate to a homomorphism $\Gamma_F \xrightarrow{\rho'} H_\alpha(R)$ with the resulting composite

$$\Gamma_F \xrightarrow{\rho'} H_\alpha(R) \xrightarrow{\mathrm{Ad}} \mathrm{GL}(\mathfrak{g}_\alpha \otimes R) = R^\times$$

equal to κ.

We shall call such a ρ to be of Ramakrishna type α as well. We denote by $\mathrm{Def}_{\bar{\rho}}^{\mathrm{Ram}}$ the corresponding deformation functor.

The following lemma is [loc. cit., Lemma 4.10].

Lemma 3.2. $\mathrm{Lift}_{\bar{\rho}}^{\mathrm{Ram}}$ *is well defined and smooth.*

Consider the subtorus $T_\alpha = \mathrm{Ker}(\alpha)^0$ of T, and denote by $\mathfrak{t}_\alpha$ its Lie algebra. There is a canonical decomposition $\mathfrak{t}_\alpha \oplus \mathfrak{l}_\alpha = \mathfrak{t}$ with $\mathfrak{l}_\alpha$ the one-dimensional torus generated by the coroot $\alpha^\vee$.

The next lemma [loc. cit., Lemma 4.11] is crucial in the global deformation theory.

Lemma 3.3. *Assume $\bar{\rho}$ is of Ramakrishna type α. Let $W = \mathfrak{t}_\alpha \oplus \mathfrak{g}_\alpha$, and let $W^\perp$ be the annihilator of W under the Killing form on $\mathfrak{g}$. Let $L_{\bar{\rho}}^{\mathrm{Ram}}$ and $L_{\bar{\rho}}^{\mathrm{Ram},\perp}$ be the tangent space of $\mathrm{Def}_{\bar{\rho}}^{\mathrm{Ram}}$ and the annihilator of $L_{\bar{\rho}}^{\mathrm{Ram}}$ under the local duality pairing, respectively. Then:*

(1) $L_{\bar{\rho}}^{\mathrm{Ram}} \cong H^1(\Gamma_F, \bar{\rho}(W))$.

(2) $\dim L_{\bar{\rho}}^{\mathrm{Ram}} = h^0(\Gamma_F, \bar{\rho}(\mathfrak{g}))$.

(3) $L_{\bar{\rho}}^{\mathrm{Ram},\perp} \cong H^1(\Gamma_F, \bar{\rho}(W^\perp)(1))$.

(4) *Let $L_{\bar{\rho}}^{\mathrm{Ram},\square}$ and $L_{\bar{\rho}}^{\mathrm{Ram},\perp,\square}$ be the preimages in $Z^1(\Gamma_F, \bar{\rho}(\mathfrak{g}))$ of $L_{\bar{\rho}}^{\mathrm{Ram}}$ and $L_{\bar{\rho}}^{\mathrm{Ram},\perp}$, respectively. Under the canonical decomposition*

$$\mathfrak{g} = \bigoplus_\gamma \mathfrak{g}_\gamma \oplus \mathfrak{t}_\alpha \oplus \mathfrak{l}_\alpha,$$

all cocycles in $L_{\bar{\rho}}^{\mathrm{Ram},\square}$ and $L_{\bar{\rho}}^{\mathrm{Ram},\perp,\square}$ have $\mathfrak{l}_\alpha$ and $\mathfrak{g}_{-\alpha}$ components equal to zero, respectively.

3A2. *The global argument.* In this section, we assume G is semisimple. Let $\bar{\rho} : \Gamma_{\mathbb{Q},S} \to G(k)$ be a continuous homomorphism for which $h^0(\Gamma_{\mathbb{Q}}, \bar{\rho}(\mathfrak{g})) = h^0(\Gamma_{\mathbb{Q}}, \bar{\rho}(\mathfrak{g})(1)) = 0$. In particular, the deformation functor is representable. The following theorem is proved in [Patrikis 2016, Proposition 5.2]. For a review on global deformation theory and systems of Selmer groups, see [Patrikis 2016, Sections 3.2–3.3].

Theorem 3.4. *Suppose that there is a global deformation condition $\mathcal{L} = \{L_v\}_{v \in S}$ consisting of* smooth *local deformation conditions for each place $v \in S$. Let $K = \mathbb{Q}(\bar{\rho}(\mathfrak{g}), \mu_l)$. We assume the following:*

(1)
$$\sum_{v \in S}(\dim L_v) \geq \sum_{v \in S} h^0(\Gamma_{\mathbb{Q}_v}, \bar{\rho}(\mathfrak{g})).$$

(2) $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g}))$ *and* $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g})(1))$ *vanish.*

(3) *Assume item (2) holds. For any pair of nonzero Selmer classes $\phi \in H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g})(1))$ and $\psi \in H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g}))$, we can restrict them to Γ_K where they become homomorphisms, which are nonzero by item (2). Letting K_ϕ/K and K_ψ/K be their fixed fields, we assume that K_ϕ and K_ψ are linearly disjoint over K.*

(4) *Consider any ϕ and ψ as in the hypothesis of item (3). There exists an element $\sigma \in \Gamma_{\mathbb{Q}}$ such that $\bar{\rho}(\sigma)$ is a regular semisimple element of G, the connected component of whose centralizer we denote T, and such that there exists a root $\alpha \in \Phi(G, T)$ satisfying*

   (a) $\alpha(\bar{\rho}(\sigma)) = \bar{\kappa}(\sigma)$,
   (b) $k[\psi(\Gamma_K)]$ *has an element with nonzero $\mathfrak{l}_\alpha$ component, and*
   (c) $k[\phi(\Gamma_K)]$ *has an element with nonzero $\mathfrak{g}_{-\alpha}$ component.*

Then there exists a finite set of primes Q disjoint from S, and a lift $\rho : \Gamma_{\mathbb{Q},S \cup Q} \to G(\mathcal{O})$ of $\bar{\rho}$ such that ρ is of type L_v at all $v \in S$ and of Ramakrishna type at all $v \in Q$.

Proof. We sketch the proof for the reader's convenience. By the arguments in [Taylor 2003, Lemma 1.1] (which carry without modification to other groups) it suffices to enlarge $\mathcal{L}$ to make the dual Selmer group

$H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar\rho(\mathfrak{g})(1))$ vanish. We may assume the dual Selmer group is nontrivial and take a nonzero class ϕ in it. Item (1) implies by Wiles' formula (Proposition 4.10) that $H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar\rho(\mathfrak{g}))$ is nontrivial. So we can take a nonzero class ψ in it. Item (3), (4) and Chebotarev's density theorem all together imply there exists infinitely many $w \notin S$ such that $\psi \mid w \notin L^{\mathrm{Ram}}_{\bar\rho \mid w}$ and $\phi \mid w \notin L^{\mathrm{Ram},\perp}_{\bar\rho \mid w}$. In particular, we have

$$\psi \notin H^1_{\mathcal{L} \cup L^{\mathrm{Ram}}_{\bar\rho \mid w}}(\Gamma_{\mathbb{Q}, S \cup w}, \bar\rho(\mathfrak{g})), \tag{1}$$

and

$$\phi \notin H^1_{\mathcal{L}^\perp \cup L^{\mathrm{Ram},\perp}_{\bar\rho \mid w}}(\Gamma_{\mathbb{Q}, S \cup w}, \bar\rho(\mathfrak{g})(1)). \tag{2}$$

If we can show

$$H^1_{\mathcal{L}^\perp \cup L^{\mathrm{Ram},\perp}_{\bar\rho \mid w}}(\Gamma_{\mathbb{Q}, S \cup w}, \bar\rho(\mathfrak{g})(1)) \subset H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q}, S}, \bar\rho(\mathfrak{g})(1)), \tag{3}$$

then (2) will imply that (3) is a strict inclusion. The key point now is that if we let L^{unr}_w denote the unramified cohomology at w, then $L_w = L^{\mathrm{unr}}_w \cap L^{\mathrm{Ram}}_{\bar\rho \mid w}$ is codimension one in L^{unr}_w, which, together with a double invocation of Wiles' formula and (1), implies

$$H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar\rho(\mathfrak{g})(1)) = H^1_{\mathcal{L}^\perp \cup L^\perp_w}(\Gamma_{\mathbb{Q}, S \cup w}, \bar\rho(\mathfrak{g})(1)),$$

from which (3) follows. A variation of this argument can be found in the proof of Proposition 3.13. Now for the new Selmer system, item 1 still holds (Lemma 3.3(2)). So we can apply the above argument finitely many times until the dual Selmer group of the enlarged Selmer system vanishes. $\qquad\square$

3B. *A variant of the global argument.* In this section, we let G be a simple algebraic group and let $\bar\rho : \Gamma_{\mathbb{Q}} \to G(k)$ be as in Section 2A. Recall that $\bar\rho(\Gamma_{\mathbb{Q}})$ is a subgroup of $N_G(T)_k$. For $l = \mathrm{char}(k)$ large enough, $\bar\rho(\mathfrak{g})$ decomposes into the sum of $\bar\rho(\mathfrak{t})$ and another one or two summands depending on whether or not $\Phi(G, T)$ is simply laced; see Propositions 2.9, 2.11, 2.13 and 2.17. We fix a Selmer system $\mathcal{L}$.

Proposition 3.5. *Assume that l is large enough. Then items* (2) *and* (3) *in Theorem 3.4 are satisfied.*

Proof. For item (2), note that $|\mathrm{Gal}(K/\mathbb{Q})|$ divides $(l-1)|\bar\rho(\Gamma_{\mathbb{Q}})|$, which is prime to l by the construction of $\bar\rho$. Since the coefficients field k of H^1 has characteristic l, this implies the vanishing of H^1.

For item (3), since $\psi : \mathrm{Gal}(K_\psi/K) \cong \psi(\Gamma_K)$ and $\phi : \mathrm{Gal}(K_\phi/K) \cong \phi(\Gamma_K)$ are $\mathrm{Gal}(K/\mathbb{Q})$-equivariant isomorphisms, it is enough to check that the irreducible summands in $\mathfrak{g}$ and $\mathfrak{g}(1)$ are nonisomorphic. We check this case by case. If G is of type A_n or D_n, by the construction of $\bar\rho$, the alternating group A_{n+1} or A_n, respectively, may be identified with a subgroup of $\bar\rho(\Gamma_{\mathbb{Q}})$. We take an element $\sigma \in \Gamma_{\mathbb{Q}}$ such that $\bar\rho(\sigma) \in A_n$ has order 2. Since $\mathbb{Q}(\bar\rho)$ (the fixed field of $\bar\rho$) is unramified at l, $\mathbb{Q}(\bar\rho)$ and $\mathbb{Q}(\mu_l)$ are linearly disjoint over $\mathbb{Q}$, so we may modify σ if necessary to make $\bar\kappa(\sigma) \neq 1$. Consider the eigenvalues of σ on $\mathfrak{t}$ and $\mathfrak{t}(1)$ (here we recall that $\mathfrak{t}$ is the Lie algebra of the maximal split torus T of G in the construction of $\bar\rho$); the eigenvalues on $\mathfrak{t}$ are ± 1, whereas none of the eigenvalues on $\mathfrak{t}(1)$ can be 1 or -1. Thus $\mathfrak{t}$ is not isomorphic to $\mathfrak{t}(1)$ as Galois modules. On the other hand, since $T := T(k) \subset \bar\rho(\Gamma_{\mathbb{Q}})$, we can find $\tau \in \Gamma_{\mathbb{Q}}$ such that $\bar\rho(\tau)$ is a regular semisimple element for which $\alpha(\bar\rho(\tau)) = a$ for $\alpha \in \Delta$, where a is a generator of $(\mathbb{Z}/l\mathbb{Z})^\times$ and Δ is a fixed set of simple roots in Φ. Again since $\mathbb{Q}(\bar\rho)$ and $\mathbb{Q}(\mu_l)$ are linearly

disjoint over $\mathbb{Q}$, we may modify τ if necessary to make $\bar{\kappa}(\tau) = a$. Consider the eigenvalues of τ on $\mathfrak{g}_\Phi$ and $\mathfrak{g}_\Phi(1)$, those on $\mathfrak{g}_\Phi$ are $\{\alpha(\bar{\rho}(\tau)) : \alpha \in \Phi\}$, whereas those on $\mathfrak{g}_\Phi(1)$ are $\{a \cdot \alpha(\bar{\rho}(\tau)) : \alpha \in \Phi\}$. Note that $\alpha(\bar{\rho}(\tau)) = a^{\mathrm{ht}(\alpha)}$ and the order of a is $l-1$, it is clear that these two sets are different when l is large enough. Thus, $\mathfrak{g}_\Phi$ and $\mathfrak{g}_\Phi(1)$ are nonisomorphic as Galois modules.

If G is of type B_n, by the construction of $\bar{\rho}$, the alternating group A_n may be identified with a subgroup of $\bar{\rho}(\Gamma_\mathbb{Q})$. Using the argument in the previous paragraph, we see that $\mathfrak{t}$ is not isomorphic to $\mathfrak{t}(1)$ as Galois modules. On the other hand, we need to show that $\bar{\rho}(\mathfrak{g}_l), \bar{\rho}(\mathfrak{g}_s), \bar{\rho}(\mathfrak{g}_l)(1), \bar{\rho}(\mathfrak{g}_s)(1)$ are pairwise nonisomorphic as Galois modules. Just like before we can find $\tau \in \Gamma_\mathbb{Q}$ such that $\bar{\rho}(\tau)$ is a regular semisimple element for which $\alpha(\bar{\rho}(\tau)) = a$ for $\alpha \in \Delta$ and $\bar{\kappa}(\tau) = a$, where a is a generator of $(\mathbb{Z}/l\mathbb{Z})^\times$ and Δ is a fixed set of simple roots in Φ. Since l is large enough, the sets $\{\alpha(\bar{\rho}(\tau)) : \alpha \in \Phi_l\}$, $\{\alpha(\bar{\rho}(\tau)) : \alpha \in \Phi_s\}$, $\{a \cdot \alpha(\bar{\rho}(\tau)) : \alpha \in \Phi_l\}$ and $\{a \cdot \alpha(\bar{\rho}(\tau)) : \alpha \in \Phi_s\}$ must be distinct. So τ has different eigenvalues on $\bar{\rho}(\mathfrak{g}_l), \bar{\rho}(\mathfrak{g}_s), \bar{\rho}(\mathfrak{g}_l)(1), \bar{\rho}(\mathfrak{g}_s)(1)$ and hence they are pairwise nonisomorphic Galois modules.

The demonstrations are the same for type C_n and E_7. □

Let M be a finite dimensional k-vector space with a continuous $\Gamma_\mathbb{Q}$-action. Define its *Tate dual* to be the space $M^\vee = \mathrm{Hom}(M, \mu_\infty)$ equipped with the following $\Gamma_\mathbb{Q}$-action:

$$(\sigma f)(m) := \sigma(f(\sigma^{-1}m)).$$

Proposition 3.6. *For any continuous homomorphism $\bar{\rho} : \Gamma_\mathbb{Q} \to G(k)$, $\bar{\rho}(\mathfrak{g})^\vee \cong \bar{\rho}(\mathfrak{g})(1)$. For $\bar{\rho}$ as in Section 2A, $\bar{\rho}(\mathfrak{t})^\vee \cong \bar{\rho}(\mathfrak{t})(1)$.*

Proof. As l is sufficiently large, the killing form is a nondegenerate G-invariant symmetric bilinear form on $\mathfrak{g}$, which identifies the contragredient representation $\mathfrak{g}^*$ with $\mathfrak{g}$, and hence identifies $\bar{\rho}(\mathfrak{g})^\vee$ with $\bar{\rho}(\mathfrak{g})(1)$ as Galois modules. If $\bar{\rho}$ is as in Section 2A, then the Galois action on $\mathfrak{t}$ factors through W. It is easy to see that the standard bilinear form on $\mathfrak{t}$ is nondegenerate and W-invariant. Just as above, we deduce that $\bar{\rho}(\mathfrak{t})^\vee \cong \bar{\rho}(\mathfrak{t})(1)$ as Galois modules. □

Definition 3.7. Let $\mathcal{L} = \{L_v\}_{v \in S}$ be the Selmer system corresponding to a global deformation condition for $\bar{\rho}$ that is unramified outside a finite set of places S, and let $\mathcal{L}^\perp = \{L_v^\perp\}_{v \in S}$ be the associated dual Selmer system. Define the *M-Selmer group* as follows:

$$H^1_\mathcal{L}(\Gamma_S, M) = \mathrm{Ker}\left(H^1(\Gamma_S, M) \to \bigoplus_{v \in S} H^1(\Gamma_v, M)/(L_v \cap H^1(\Gamma_v, M))\right),$$

and define the *M-dual Selmer group* as follows:

$$H^1_{\mathcal{L}^\perp}(\Gamma_S, M^\vee) = \mathrm{Ker}\left(H^1(\Gamma_S, M^\vee) \to \bigoplus_{v \in S} H^1(\Gamma_v, M^\vee)/(L_v^\perp \cap H^1(\Gamma_v, M^\vee))\right).$$

To apply Theorem 3.4, we need to make sure that items (1)–(4) in it are satisfied. By choosing an appropriate $\mathcal{L}$, we can make item (1) hold. Items (2) and (3) are satisfied by Proposition 3.5. It is tricky to deal with item (4): the images of ϕ and ψ, which are $\Gamma_\mathbb{Q}$-submodules of $\bar{\rho}(\mathfrak{g})$, must satisfy the group-theoretic properties in (b) and (c); if we can find an element σ as in item (4) such that *all* summands

of $\bar{\rho}(\mathfrak{g})$ satisfies these properties, then item (4) will be satisfied. So achieving item (4) crucially depends on the group-theoretic properties of submodules of $\bar{\rho}(\mathfrak{g})$. We need to find a regular semisimple element Σ in $\bar{\rho}(\Gamma_{\mathbb{Q}})$, the connected component of whose centralizer we denote T', for which there exists a root $\alpha' \in \Phi' := \Phi(G, T')$ such that:

(1) $\alpha'(\Sigma) \in (\mathbb{Z}/l\mathbb{Z})^{\times}$,

(2) Every irreducible summand of $\bar{\rho}(\mathfrak{g})$ has an element with nonzero $\mathfrak{l}_{\alpha'}$ component.

(3) Every irreducible summand of $\bar{\rho}(\mathfrak{g})$ has an element with nonzero $\mathfrak{g}_{-\alpha'}$ component.

Unfortunately, for our residual representation, there is no such element which meets all three conditions. The rest of this section will show how item (4) of Theorem 3.4 can be met by controlling $\psi(\Gamma_K)$ for a given class ψ in the Selmer group.

If we take a regular semisimple element Σ in T (which is the fixed split maximal torus of $G(k)$ we use when constructing the residual representation), then there is no $\alpha \in \Phi$ fulfilling both (2) and (3). Instead, we look for $\Sigma \in N = N_G(T)$ for which $\pi(\Sigma)$ is a nontrivial element in W, where $\pi : N_G(T) \twoheadrightarrow \mathcal{W}$ is the canonical quotient map.

Lemma 3.8. *Assume the characteristic of k is large enough for G. Then for any $w \in \mathcal{W}$ that fixes a noncentral element of $\mathrm{Lie}(T)$, there exist a regular semisimple element $n \in N$ (regular with respect to G) such that $\pi(n) = w$. If G is of type A_1, A_2, B_2, C_2, then for any $w \in \mathcal{W}$, there exist a regular semisimple element $n \in N$ (regular with respect to G) such that $\pi(n) = w$.*

Proof. The second part follows from a straightforward calculation. We will prove the first part. We first make the following observation: if M is a Levi subgroup of G, then (by looking at the action of simple roots outside M on elements of $Z_G(M)^0$) for every M-regular semisimple element $t \in M$, there is a G-regular semisimple element of $t Z_G(M)^0$. If w fixes a noncentral element of $\mathrm{Lie}(T)$, then we take M to be $Z_G(\mathrm{Lie}(T)^w)$, which is a proper Levi subgroup of G since the characteristic of k is large enough for G. By induction on the semisimple rank, there is a M-regular semisimple element n' such that $\pi(n') = w$, so there is a G-regular semisimple element $n = n'z$ with $z \in Z_G(M)^0$, and hence $\pi(n) = \pi(n'z) = \pi(n')\pi(z) = \pi(n') = w$. $\qquad\square$

Remark 3.9. The above lemma should be true without assuming w fixes a noncentral element of $\mathrm{Lie}(T)$, but the author does not know how to remove this assumption. For GL_n, one can show that (by matrix calculations) the property holds for all $w \in S_n$ as long as the characteristic of k is large enough.

Let t' be a regular semisimple element in G and $t \in T$ be an element that is conjugate to t'. Then t and t' determine a unique bijection between $\Phi = \Phi(G, T)$ and $\Phi' = \Phi(G, T')$ with $T' = Z_G(t')^0$: for any $\alpha \in \Phi$, define $\alpha' \in \Phi'$ such that

$$\alpha'(h) = \alpha(g^{-1}hg)$$

for any $h \in T'$, where g is an element in G such that $g^{-1}t'g = t$. Since t is regular semisimple, α' is independent of g.

Recall that for $\alpha \in \Phi$, s_α is the simple reflection in the Weyl group of Φ associated to α.

Lemma 3.10. *Assume the characteristic of k is not 2. For a long root $\alpha \in \Phi$, let Σ be a regular semisimple element in N such that $\pi(\Sigma) = s_\alpha$ (which exists by Lemma 3.8). We fix an element $t \in T$ that is conjugate to Σ and let $T' = Z_G(\Sigma)^0$. The elements Σ and t determine a bijection between Φ and Φ' as above.*

- *If Φ is of type A_n ($n \geq 1$) or D_n ($n \geq 4$), then the root $\alpha' \in \Phi'$ corresponding to α fulfills (1) and (3). For (2), $\mathfrak{g}_\Phi$ (recall that $\mathfrak{g}_\Phi := \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha$) has an element with nonzero $\mathfrak{l}_{\alpha'}$ component, but t does not.*

- *If Φ is of type B_n, C_n ($n \geq 2$) or E_7, then α' fulfills (1) and t has a vector with nonzero $\mathfrak{g}_{-\alpha'}$ component.*

Moreover, $\mathfrak{t}' \cap \mathfrak{t} = \mathfrak{t}'_{\alpha'} \cap \mathfrak{t} = W \cap \mathfrak{t}$, where $W = \mathfrak{t}'_{\alpha'} \oplus \mathfrak{g}_{\alpha'}$.

Proof. It is clear that $\alpha'(\Sigma) = -1$, so (1) is satisfied. We need to show:

- The space $\mathfrak{l}_\alpha$ has nonzero $\mathfrak{g}_{-\alpha'}$ component.

- The space $\mathfrak{g}_\alpha$ has nonzero $\mathfrak{l}_{\alpha'}$ and $\mathfrak{g}_{-\alpha'}$ component.

- $\mathfrak{t}' \cap \mathfrak{t} = \mathfrak{t}'_{\alpha'} \cap \mathfrak{t} = W \cap \mathfrak{t}$.

This is essentially a GL_2-calculation. We may perform the calculation in the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\alpha$, whose root lattice is isomorphic to $\{x_1 e_1 + x_2 e_2 \mid x_i \in \mathbb{Z}, x_1 + x_2 = 0\}$. We take $\alpha = e_1 - e_2$ with the corresponding root vector

$$X_\alpha := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

We have $\Sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Then $P^{-1} \Sigma P = \mathrm{diag}(1, -1)$. The first bullet follows from the identity

$$P^{-1} \cdot \mathrm{diag}(h_1, h_2) \cdot P = -\frac{1}{2} \begin{pmatrix} -h_1 - h_2 & -h_1 + h_2 \\ -h_1 + h_2 & -h_1 - h_2 \end{pmatrix}.$$

The second bullet follows from the identity

$$P^{-1} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} P = -\frac{1}{2} \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}.$$

To show the third bullet, note that elements in $\mathfrak{t}'$ are of the form $\begin{pmatrix} h & k \\ k & h \end{pmatrix}$, elements in $\mathfrak{t}'_{\alpha'}$ are of the form $\begin{pmatrix} h & 0 \\ 0 & h \end{pmatrix}$, and elements in $\mathfrak{g}_{\alpha'}$ are of the form $\begin{pmatrix} x & -x \\ x & -x \end{pmatrix}$. It follows that all three intersections in the third bullet are the one dimensional k-vector space spanned by $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $\qquad\square$

Lemma 3.11. *Suppose the characteristic of k is not 2 or 3. Assume that Φ is of type B_n, C_n ($n \geq 2$) or E_7, so $\bar{\rho}(\mathfrak{g}) = \bar{\rho}(\mathfrak{t}) \oplus \bar{\rho}(\mathfrak{g}_l) \oplus \bar{\rho}(\mathfrak{g}_s)$ for B_n and C_n, and $\bar{\rho}(\mathfrak{g}) = \bar{\rho}(\mathfrak{t}) \oplus \bar{\rho}(\mathfrak{g}_a) \oplus \bar{\rho}(\mathfrak{g}_b)$ for E_7 (see Section 2A4-2A6).*

(1) *(Type B_n and C_n) For a pair of nonperpendicular $\beta, \gamma \in \Phi$ with β long and γ short, let Σ be a regular semisimple element in N such that $\pi(\Sigma) = s_\beta \cdot s_\gamma$ (which exists by Lemma 3.8). We fix an element $t \in T$ that is conjugate to Σ and let $T' = Z_G(\Sigma)^0$. The elements Σ and t determine a*

bijection between Φ and $\Phi' = \Phi(G, T')$. Then for all long root α' in the span of β' and γ' (which is a subsystem of Φ' of type C_2), (3) is satisfied. For (2), $\mathfrak{g}_l$ and $\mathfrak{g}_s$ have elements with nonzero $\mathfrak{l}_{\alpha'}$ component, but $\mathfrak{t}$ does not. The element $\alpha'(\Sigma)$ has order 4 in $\bar{k}^\times$, hence (1) is satisfied only for $l \equiv 1(4)$.

(2) *(Type E_7) For a pair of nonperpendicular $\beta, \gamma \in \Phi$ with $\mathfrak{g}_\beta \subset \mathfrak{g}_a$ and $\mathfrak{g}_\gamma \subset \mathfrak{g}_b$, let Σ be a regular semisimple element in N such that $\pi(\Sigma) = s_\beta \cdot s_\gamma$. We fix an element $\mathfrak{t} \in T$ that is conjugate to Σ and let $T' = Z_G(\Sigma)^0$. The elements Σ and $\mathfrak{t}$ determine a bijection between Φ and $\Phi' = \Phi(G, T')$. Then for all roots α' in the span of β' and γ' (which is a subsystem of Φ' of type A_2), (3) is satisfied. For (2), $\mathfrak{g}_a$ and $\mathfrak{g}_b$ have elements with nonzero $\mathfrak{l}_{\alpha'}$ component, but $\mathfrak{t}$ does not. The elements $\alpha'(\Sigma)$ has order 3 in $\bar{k}^\times$, hence (1) is satisfied only for $l \equiv 1(3)$.*

Moreover, $W \cap \mathfrak{t} \subset \mathfrak{t}'$, where $W = \mathfrak{t}'_{\alpha'} \oplus \mathfrak{g}_{\alpha'}$.

Proof. We first prove (2). Let α' be any root in the span of β' and γ'. We need to show:

- $\mathfrak{l}_\beta \oplus \mathfrak{l}_\gamma$ has nonzero $\mathfrak{g}_{-\alpha'}$ component.
- $\mathfrak{g}_\beta$ and $\mathfrak{g}_\gamma$ have nonzero $\mathfrak{l}_{\alpha'}$ component and nonzero $\mathfrak{g}_{-\alpha'}$ component.
- $W \cap \mathfrak{t} \subset \mathfrak{t}'$.

We may perform the calculation in the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\beta$ and $\mathfrak{g}_\gamma$, whose root lattice is isomorphic to $\{x_1 e_1 + x_2 e_2 + x_3 e_3 \mid x_i \in \mathbb{Z}, x_1 + x_2 + x_3 = 0\}$. We take $\beta = e_1 - e_2, \gamma = e_2 - e_3$ with the corresponding root vectors

$$X_\beta := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad X_\gamma := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

We have

$$\Sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let r be a (fixed) primitive 3-rd root of unity in $\bar{k}$, and let

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & r^2 & r \\ 1 & r & r^2 \end{pmatrix},$$

then

$$P^{-1} \Sigma P = \mathrm{diag}(1, r, r^2),$$

which implies $\alpha'(\Sigma)$ has order 3 in $\bar{k}^\times$. We have $P^{-1} \mathrm{diag}(a, b, c) P$ is a nonzero scalar multiple of

$$\begin{pmatrix} ar + br + cr & ar + b + cr^2 & ar + br^2 + c \\ ar + br^2 + c & ar + br + cr & ar + b + cr^2 \\ ar + b + cr^2 & ar + br^2 + c & ar + br + cr \end{pmatrix},$$

from which the first bullet follows. On the other hand, we have $P^{-1}X_\beta P$ is a nonzero scalar multiple of

$$
\begin{pmatrix} r & 1 & r^2 \\ r & 1 & r^2 \\ r & 1 & r^2 \end{pmatrix},
$$

from which it follows that $\mathfrak{g}_\beta$ has nonzero $\mathfrak{l}_{\alpha'}$ component and nonzero $\mathfrak{g}_{-\alpha'}$ component for any α'. Similarly, $\mathfrak{g}_\gamma$ has nonzero $\mathfrak{l}_{\alpha'}$ component and nonzero $\mathfrak{g}_{-\alpha'}$ component for any α'. The second bullet follows. We now show the third bullet for $\alpha' = \beta'$, the calculation is similar for other roots. We have

$$
P \begin{pmatrix} a & x & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix} P^{-1}
$$

is a nonzero constant multiple of

$$
\begin{pmatrix} 2ar + br + xr & -a+b+xr^2 & -ar^2+br^2+x \\ -ar^2+br^2+xr & br+xr^2 & -a+b+x \\ -a+b+xr & -ar^2+br^2+xr^2 & 2ar+br+x \end{pmatrix}.
$$

A simple calculation shows demanding the off-diagonal entries in the above matrix to be zero will force all of a, b, x to be zero. Thus $W \cap \mathfrak{t}$ is trivial in the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\beta$ and $\mathfrak{g}_\gamma$. It follows that $W \cap \mathfrak{t}$ is contained in $\mathfrak{t}'$.

The proof of (1) is very similar to that of (2). The computation may be performed in the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\beta$ and $\mathfrak{g}_\gamma$, which is of type C_2. Let α' be a long root in the span of β' and γ'. We will show the three bullets above are true. The roots are $\{\pm(e_1 - e_2), \pm(e_1 + e_2), \pm2e_1, \pm2e_2\}$. We fix an alternating form $x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1$ on k^2 and let $\beta = e_1 - e_2$ and $\gamma = 2e_1$ with corresponding root vectors

$$
X_\beta := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad X_\gamma := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.
$$

We have

$$
\Sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.
$$

Let r be a (fixed) primitive eighth root of unity in $\bar{k}$, and let

$$
P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ r & r^3 & r^5 & r^7 \\ r^3 & r & r^7 & r^5 \\ r^2 & r^6 & r^2 & r^6 \end{pmatrix},
$$

then
$$P^{-1}\Sigma P = \mathrm{diag}(r, r^3, r^5, r^7),$$

which implies $\alpha'(\Sigma)$ has order 4 in $\bar{k}^\times$. We have $P^{-1}\mathrm{diag}(a, b, -b, -a)P$ is a nonzero scalar multiple of

$$\begin{pmatrix} 0 & a - br^6 & 0 & a - br^2 \\ a - br^6 & 0 & a + br^2 & 0 \\ 0 & a + br^6 & 0 & a + br^2 \\ a - br^6 & 0 & a - br^2 & 0 \end{pmatrix}.$$

Let $\alpha' \in \Phi'$ be any long root, then α' satisfies the first bullet. On the other hand, $P^{-1}X_\beta P$ is a nonzero scalar multiple of

$$\begin{pmatrix} r - r^7 & 0 & r^5 - r^7 & r^7 - r^3 \\ 0 & r^3 + r & 2r^5 & r^7 + r \\ r + r^7 & 2r^3 & r^5 + r^7 & 0 \\ r - r^5 & r^3 - r & 0 & r^7 - r \end{pmatrix},$$

and $P^{-1}X_\gamma P$ is a nonzero scalar multiple of

$$\begin{pmatrix} r^2 & r^6 & r^2 & r^6 \\ r^2 & r^6 & r^2 & r^6 \\ r^2 & r^6 & r^2 & r^6 \\ r^2 & r^6 & r^2 & r^6 \end{pmatrix},$$

from which the second bullet follows. We check the third bullet for α' corresponding to $2e_2$, the calculation is similar for other long roots in Φ'. We have

$$P \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -a \end{pmatrix} P^{-1}$$

is a nonzero scalar multiple of

$$\begin{pmatrix} x & a(r^5 - r^3) + xr^3 & a(r^5 - r^3) - xr^5 & a(r^6 - r^2) + xr^6 \\ a(r - r^7) + xr^3 & r^6 x & 2ar^6 - x & a(r^5 - r^3) + xr \\ a(r^3 - r^5) + xr & 2ar^2 - x & -r^6 x & a(r^3 - r^5) + xr^7 \\ -2ar^6 + xr^6 & a(r^3 - r^5) + xr & a(r^7 - r) - xr^3 & -x \end{pmatrix}.$$

It is easy to see that for the matrix to be diagonal, both of a and x have to be zero. Thus $W \cap \mathfrak{t}$ is trivial in the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\beta$ and $\mathfrak{g}_\gamma$. It follows that $W \cap \mathfrak{t}$ is contained in $\mathfrak{t}'$. $\qquad\square$

Let Σ, α' be as in Lemma 3.10, (1) for Φ of type A_n or D_n, and Lemma 3.11 for Φ of type B_n, C_n or E_7. We have $\alpha(\Sigma) \in (\mathbb{Z}/l\mathbb{Z})^\times$ for primes l satisfying an appropriate congruence condition if necessary. We need to modify the element Σ to make it land in $\bar{\rho}(\Gamma_{\mathbb{Q}})$. When Φ is of type A_n or D_n, $\pi(\bar{\rho}(\Gamma_{\mathbb{Q}})) = [\mathcal{W}, \mathcal{W}]$ (see 2.1.3 and 2.1.5). For any $\alpha \in \Phi$, we write $\mathfrak{sl}_2^\alpha$ for the Lie subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$. We replace s_α by $s_\alpha s_\beta$ for some root β orthogonal to α such that $[\mathfrak{sl}_2^\alpha, \mathfrak{sl}_2^\beta]$ is trivial (such β exists because

$n \geq 4$) and replace Σ with a regular semisimple element in $N_G(T)$ that maps to $s_\alpha s_\beta$ when modulo $T(k)$. Note that $s_\alpha s_\beta \in [\mathcal{W}, \mathcal{W}]$: The Weyl group $\mathcal{W}$ acts transitively on the irreducible root system Φ, so there exists $w \in \mathcal{W}$ such that $w\alpha = \beta$, and hence $ws_\alpha w^{-1} = s_\beta$; it follows that $s_\alpha s_\beta = [s_\alpha, w]$. We again denote this new element by Σ, which now lands in $\bar{\rho}(\Gamma_{\mathbb{Q}})$. Lemma 3.10(1) still holds. When Φ is of type B_n, we again have $\pi(\bar{\rho}(\Gamma_{\mathbb{Q}})) = [\mathcal{W}, \mathcal{W}]$ (see 2.1.5). As $s_\beta s_\gamma \in [\mathcal{W}, \mathcal{W}]$, $\Sigma \in \bar{\rho}(\Gamma_{\mathbb{Q}})$, so no modification is needed. When Φ is of type C_n, $\pi(\bar{\rho}(\Gamma_{\mathbb{Q}})) = \mathcal{W}$ (see 2.1.4), so we automatically have $\Sigma \in \bar{\rho}(\Gamma_{\mathbb{Q}})$. When Φ is of type E_7, the corresponding element Σ is in $\bar{\rho}(\Gamma_{\mathbb{Q}})$ as well (see 2.1.6). Since $\bar{\rho}$ is unramified at l and $\mathbb{Q}(\mu_l)$ is totally ramified at l, $\mathbb{Q}(\bar{\rho})$ and $\mathbb{Q}(\mu_l)$ are linearly disjoint over $\mathbb{Q}$. So there exists an element $\sigma \in \Gamma_{\mathbb{Q}}$ such that $\bar{\rho}(\sigma) = \Sigma$ and $\bar{\kappa}(\sigma) = \alpha'(\Sigma)$. It follows that $\alpha'(\bar{\rho}(\sigma)) = \bar{\kappa}(\sigma)$.

Lemma 3.12. *Suppose there is a Selmer system $\mathcal{L} = \{L_v\}_{v \in S}$ for which the $\mathfrak{t}$-Selmer group $H^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t}))$ is trivial. We take a pair of nonzero Selmer classes $\phi \in H^1_{\mathcal{L}^\perp}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g})(1))$ and $\psi \in H^1_{\mathcal{L}}(\Gamma_{\mathbb{Q},S}, \bar{\rho}(\mathfrak{g}))$. Then item* (4) *of Theorem 3.4 is satisfied.*

Proof. We need to check Theorem 3.4(4)(b) and (c). First, Proposition 3.5 and the inflation-restriction sequence imply that $\psi(\Gamma_K)$ and $\phi(\Gamma_K)$ are nontrivial. By Lemmas 3.10 and 3.11, every irreducible summand of $\bar{\rho}(\mathfrak{g})$ has an element with nonzero $\mathfrak{g}_{-\alpha'}$ component. In particular, (c) holds. As $H^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t}))$ is trivial, $\psi(\Gamma_K) \not\subseteq \mathfrak{t}$, which implies that $k[\psi(\Gamma_K)]$ contains $\mathfrak{g}_\Phi$ when Φ is of type A_n or D_n, $k[\psi(\Gamma_K)]$ contains one of $\mathfrak{g}_l$ and $\mathfrak{g}_s$ when Φ is of type B_n or C_n, and $k[\psi(\Gamma_K)]$ contains one of $\mathfrak{g}_a$ and $\mathfrak{g}_b$ when Φ is of type E_7. It then follows from Lemmas 3.10 and 3.11 that $k[\psi(\Gamma_K)]$ has an element with nonzero $\mathfrak{l}_{\alpha'}$ component. So (b) holds as well. □

The next proposition achieves the vanishing assumption of the $\mathfrak{t}$-Selmer in Lemma 3.12 by using of a variant of the cohomological arguments in Ramakrishna's method.

Proposition 3.13. *Suppose that*

$$h^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})) \leq h^1_{\mathcal{L}^\perp}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1)).$$

Then there is a finite set of places Q disjoint from S and a Ramakrishna deformation condition for each $w \in Q$ with tangent space L_w^{Ram} such that

$$H^1_{\mathcal{L} \cup \{L_w^{\mathrm{Ram}}\}_{w \in Q}}(\Gamma_{S \cup Q}, \bar{\rho}(\mathfrak{t})) = 0.$$

We may assume that $H^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t}))$ is nontrivial, for otherwise we are done. The inequality in Proposition 3.13 then implies that $H^1_{\mathcal{L}^\perp}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1))$ is nontrivial. Let $0 \neq \phi \in H^1_{\mathcal{L}^\perp}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1))$.

Lemma 3.14. *There exists $\tau \in \Gamma_{\mathbb{Q}}$ with the following properties*:

(1) $\bar{\rho}(\tau)$ *is a regular semisimple element of $G(k)$, the connected component of whose centralizer we denote T'.*

(2) *There exists $\alpha' \in \Phi(G, T')$, such that $\alpha'(\bar{\rho}(\tau)) = \bar{\kappa}(\tau)$.*

(3) $k[\phi(\Gamma_K)]$ *has an element with nonzero $\mathfrak{g}_{-\alpha'}$-component.*

Proof. We have seen that the groups $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g}))$ and $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g})(1))$ are both trivial. In particular, the groups $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{t}))$ and $H^1(\mathrm{Gal}(K/\mathbb{Q}), \bar{\rho}(\mathfrak{t})(1))$ are both trivial. The restriction-inflation sequence then implies that $\phi(\Gamma_K)$ is nontrivial. Now we let Σ, α' be as in Lemma 3.10(1) for Φ of type A_n or D_n, and Lemma 3.10(2) for Φ of type B_n, C_n or E_7. If necessary, we can modify Σ to make it land in $\bar{\rho}(\Gamma_{\mathbb{Q}})$, as explained in the paragraph preceding Lemma 3.12. We have $\alpha(\Sigma) \in (\mathbb{Z}/l\mathbb{Z})^{\times}$. Since $\bar{\rho}$ is unramified at l and $\mathbb{Q}(\mu_l)$ is totally ramified at l, $\mathbb{Q}(\bar{\rho})$ and $\mathbb{Q}(\mu_l)$ are linearly disjoint over $\mathbb{Q}$. So there exists an element $\tau \in \Gamma_{\mathbb{Q}}$ such that $\bar{\rho}(\tau) = \Sigma$ and $\bar{\kappa}(\tau) = \alpha'(\Sigma)$. It follows that $\alpha'(\bar{\rho}(\tau)) = \bar{\kappa}(\tau)$, proves (2). Statement (3) follows from Lemma 3.10. $\qquad\square$

Corollary 3.15. *There exist infinitely many places $w \notin S$ such that $\bar{\rho}|_{\Gamma_w}$ is of Ramakrishna type α' and $\phi|_{\Gamma_w} \notin L_w^{\mathrm{Ram},\perp}$.*

Proof. This follows from Lemmas 3.3, 3.14 and Chebotarev's density theorem. See the proof of [Patrikis 2016, Lemma 5.3]. $\qquad\square$

Proof of Proposition 3.13. Let w be chosen as in Corollary 3.15. We will show that

$$h^1_{\mathcal{L}^{\perp} \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)) < h^1_{\mathcal{L}^{\perp}}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1)) \tag{4}$$

and

$$h^1_{\mathcal{L} \cup L_w^{\mathrm{Ram}}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) - h^1_{\mathcal{L}^{\perp} \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)) = h^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})) - h^1_{\mathcal{L}^{\perp}}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1)) \tag{5}$$

which imply that

$$h^1_{\mathcal{L} \cup L_w^{\mathrm{Ram}}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) < h^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})),$$

from which Proposition 3.13 follows by induction.

We first show (5). By a double invocation of Wiles' formula (see Proposition 4.10), the difference between the two sides equals $\dim(L_w^{\mathrm{Ram}} \cap H^1(\Gamma_w, \bar{\rho}(\mathfrak{t}))) - h^0(\Gamma_w, \bar{\rho}(\mathfrak{t})) = h^1(\Gamma_w, \bar{\rho}(W \cap \mathfrak{t})) - h^0(\Gamma_w, \bar{\rho}(\mathfrak{t}))$. As $H^0(\Gamma_w, \bar{\rho}(\mathfrak{g})) = \mathfrak{t}'$, we have $H^0(\Gamma_w, \bar{\rho}(\mathfrak{t})) = \mathfrak{t} \cap \mathfrak{t}'$; on the other hand, the action of $\bar{\rho}(\Gamma_w)$ on $W \cap \mathfrak{t}$ is a sum of the trivial representation and the cyclotomic character. By an elementary calculation in Galois cohomology, $h^1(\Gamma_w, k) = h^1(\Gamma_w, k(1)) = 1$. It follows that $h^1(\Gamma_w, \bar{\rho}(W \cap \mathfrak{t})) = \dim W \cap \mathfrak{t}$ and so $h^1(\Gamma_w, \bar{\rho}(W \cap \mathfrak{t})) - h^0(\Gamma_w, \bar{\rho}(\mathfrak{t})) = \dim(W \cap \mathfrak{t}) - \dim(\mathfrak{t}' \cap \mathfrak{t})$, which is zero by Lemma 3.10.

It remains to prove (4). Let $L_w = L_w^{\mathrm{unr}} \cap L_w^{\mathrm{Ram}}$, so $L_w^{\perp} = L_w^{\mathrm{unr},\perp} + L_w^{\mathrm{Ram},\perp}$. We have the following obvious inclusions

$$H^1_{\mathcal{L} \cup L_w}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) \subset H^1_{\mathcal{L} \cup L_w^{\mathrm{Ram}}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})), \tag{6}$$

$$H^1_{\mathcal{L}^{\perp} \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)) \subset H^1_{\mathcal{L}^{\perp} \cup L_w^{\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)), \tag{7}$$

$$H^1_{\mathcal{L} \cup L_w}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) \subset H^1_{\mathcal{L} \cup L_w^{\mathrm{unr}}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) = H^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})), \tag{8}$$

$$H^1_{\mathcal{L}^{\perp}}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1)) = H^1_{\mathcal{L}^{\perp} \cup L_w^{\mathrm{unr},\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)) \subset H^1_{\mathcal{L}^{\perp} \cup L_w^{\perp}}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)). \tag{9}$$

As $\phi|_{\Gamma_w} \notin L_w^{\mathrm{Ram},\perp}$, (7) is a strict inclusion. We claim that (9) is an isomorphism, which will imply (4). To prove our claim, we consider (8) first. There is an exact sequence

$$0 \to H^1_{\mathcal{L} \cup L_w}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) \to H^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})) \to (L_w^{\mathrm{unr}} \cap H^1(\Gamma_w, \bar{\rho}(\mathfrak{t})))/(L_w \cap H^1(\Gamma_w, \bar{\rho}(\mathfrak{t}))).$$

As

$$L_w^{\mathrm{unr}} = H^1(\Gamma_w/I_w, \bar{\rho}(\mathfrak{g})) \xrightarrow{f \mapsto f(\mathrm{Fr}_w)} \mathfrak{g}/(\bar{\rho}(\mathrm{Fr}_w) - 1)\mathfrak{g} \cong \mathfrak{t}',$$

the top of its last term is isomorphic to $H^1(\Gamma_w, \bar{\rho}(\mathfrak{t}' \cap \mathfrak{t}))$, which has dimension $\dim(\mathfrak{t}' \cap \mathfrak{t})$; the bottom of its last term is isomorphic to $H^1(\Gamma_w, \mathfrak{t}'_\alpha \cap \mathfrak{t})$, which has dimension $\dim(\mathfrak{t}'_\alpha \cap \mathfrak{t})$. By Lemma 3.10, these dimensions are equal. So the last term is zero, and hence (8) is an isomorphism. A double invocation of Wiles' formula (Proposition 4.10) shows $h^1_{\mathcal{L}^\perp \cup L_w^\perp}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})(1)) - h^1_{\mathcal{L}^\perp}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1))$ equals

$$h^1_{\mathcal{L} \cup L_w}(\Gamma_{S \cup w}, \bar{\rho}(\mathfrak{t})) - h^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})) + h^0(\Gamma_w, \bar{\rho}(\mathfrak{t})) - \dim(L_w \cap H^1(\Gamma_w, \bar{\rho}(\mathfrak{t}))).$$

Because (8) is an isomorphism and $\dim(L_w \cap H^1(\Gamma_w, \bar{\rho}(\mathfrak{t}))) = h^1(\Gamma_w, \bar{\rho}(W \cap \mathfrak{t}' \cap \mathfrak{t})) = \dim(W \cap \mathfrak{t}' \cap \mathfrak{t}) = \dim(\mathfrak{t}' \cap \mathfrak{t}) = h^0(\Gamma_w, \bar{\rho}(\mathfrak{t}))$ (Lemma 3.10), the right hand side of the above identity is zero. Therefore, (9) is an isomorphism, which completes the proof of the proposition. □

Theorem 3.16. *Let $\mathcal{L} = \{L_v\}_{v \in S}$ be a family of smooth local deformation conditions for $\bar{\rho}$ (the residual representation defined in Section 2A) unramified outside a finite set of places S containing the real place and all places where $\bar{\rho}$ is ramified. Suppose that*

$$\sum_{v \in S} \dim L_v \geq \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g})) \quad and \quad \sum_{v \in S} \dim(L_v \cap H^1(\Gamma_v, \bar{\rho}(\mathfrak{t}))) \leq \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{t})).$$

Assume l is large enough; in addition, if Φ is of type E_7, assume $l \equiv 1(3)$, and if Φ is doubly laced, assume $l \equiv 1(4)$.

Then there is a finite set of places Q disjoint from S and a continuous lift

$$\rho : \Gamma_{S \cup Q} \to G(\mathcal{O})$$

of $\bar{\rho}$ such that ρ is of type L_v for $v \in S$ and of Ramakrishna type for $v \in Q$.

Proof. The second inequality and Wiles' formula (Proposition 4.10) imply that

$$h^1_{\mathcal{L}}(\Gamma_S, \bar{\rho}(\mathfrak{t})) \leq h^1_{\mathcal{L}^\perp}(\Gamma_S, \bar{\rho}(\mathfrak{t})(1)).$$

By Proposition 3.13, we can enlarge $\mathcal{L}$ by adding finitely many Ramakrishna deformation conditions to get a new Selmer system $\mathcal{L}' = \{L_v\}_{v \in S'}$ with $S' \supset S$ such that $H^1_{\mathcal{L}'}(\Gamma_{S'}, \bar{\rho}(\mathfrak{t})) = \{0\}$. By Lemma 3.3(2), replacing $\mathcal{L}$ by $\mathcal{L}'$ preserves the first inequality.

We choose $\sigma \in \Gamma_{\mathbb{Q}}$ and $\alpha' \in \Phi(G, T')$ as in the paragraph preceding Lemma 3.12 (this is where the congruence conditions for Φ of type B_n, C_n, E_7 come in). Chebotarev's density theorem implies that there are infinitely many places $w \notin S'$ such that $\bar{\rho}|_w$ is of Ramakrishna type α'. We have for such a prime w,

$$H^1_{\mathcal{L}' \cup L_w^{\mathrm{Ram}}}(\Gamma_{S' \cup w}, \bar{\rho}(\mathfrak{t})) = 0.$$

In other words, adding a Ramakrishna local deformation conditions does not make the $\mathfrak{t}$-Selmer group jump back to a nontrivial group. Indeed, $L_w^{\mathrm{Ram}} \cap H^1(\Gamma_w, \bar\rho(\mathfrak{t})) = H^1(\Gamma_w, \bar\rho(W \cap \mathfrak{t})) \subset H^1(\Gamma_w, \bar\rho(\mathfrak{t}' \cap \mathfrak{t})) = H^1(\Gamma_w/I_w, \bar\rho(\mathfrak{t}))$, where the middle inclusion follows from Lemma 3.10 and 3.11. So

$$H^1_{\mathcal{L}' \cup L_w^{\mathrm{Ram}}}(\Gamma_{S' \cup w}, \bar\rho(\mathfrak{t})) \subset H^1_{\mathcal{L}'}(\Gamma_{S'}, \bar\rho(\mathfrak{t})) = \{0\}.$$

Let us check the assumptions of Theorem 3.4. By Proposition 4.10 and the first inequality in the assumption, item (1) holds. Item (2) and (3) are satisfied by Proposition 3.5. As $H^1_{\mathcal{L}'}(\Gamma_{S'}, \bar\rho(\mathfrak{t})) = \{0\}$, Item (4) is satisfied by Lemma 3.12. Therefore, by the proof of Theorem 3.4, there is a strict inclusion

$$H^1_{\mathcal{L}'^{\perp} \cup L_w^{\mathrm{Ram},\perp}}(\Gamma_{\mathbb{Q}, S' \cup w}, \bar\rho(\mathfrak{g})(1)) \subset H^1_{\mathcal{L}'^{\perp}}(\Gamma_{\mathbb{Q}, S'}, \bar\rho(\mathfrak{g})(1)).$$

As the $\mathfrak{t}$-Selmer group is still trivial for the enlarged Selmer system, item (4) remains valid by Lemma 3.12. So we can find a prime $w' \notin S' \cup w$ and enlarge the Selmer system $\mathcal{L}' \cup L_w^{\mathrm{Ram}}$ in the same way so that the dual Selmer group shrinks even further. Applying this argument finitely many times, we can kill the dual Selmer group. Therefore, by the first two lines of the proof of Theorem 3.4, we obtain desired l-adic lifts. □

3C. *Deforming principal* GL_2. We use the notation in Section 2B. Recall that $\bar\rho$ is the composite $\Gamma_{\mathbb{Q}} \to \mathrm{GL}_2(k) \xrightarrow{\varphi} G(k)$ where the first map is constructed from modular forms and the second map is the principal GL_2-map.

Patrikis has shown that all simple algebraic groups of exceptional types are geometric monodromy groups for $\Gamma_{\mathbb{Q}}$ except for E_6^{ad}, E_6^{sc}, E_7^{sc} [Patrikis 2016]. In this section, we follow Patrikis' work and use the principal GL_2 to construct full-image Galois representations into E_6^{ad}, E_6^{sc}, SL_3, Spin_7.

The proof of the following theorem is identical to that of [Patrikis 2016, Theorem 7.4].

Theorem 3.17. *Let $\mathcal{L} = \{L_v\}_{v \in S}$ be a family of smooth local deformation conditions for $\bar\rho$ (the residual representation defined in Section 2B) unramified outside a finite set of places S containing the real place and all places where $\bar\rho$ is ramified. Suppose that*

$$\sum_{v \in S} \dim L_v \geq \sum_{v \in S} h^0(\Gamma_v, \bar\rho(\mathfrak{g})).$$

Assume l is large enough.

Then there is a finite set of places Q disjoint from S and a continuous lift

$$\rho : \Gamma_{S \cup Q} \to G(\mathcal{O})$$

of $\bar\rho$ such that ρ is of type L_v for $v \in S$ and of Ramakrishna type for $v \in Q$.

In [Patrikis 2016, Lemma 7.6], the following fact is verified using Magma.

Lemma 3.18. *Assume l is large enough for $\mathfrak{g}$. For $\mathfrak{g}$ of exceptional type, there is a root $\alpha \in \Phi$ such that every irreducible submodule of $\bar\rho(\mathfrak{g})$ has a vector with nonzero $\mathfrak{l}_{\alpha}$ component and a vector with nonzero $\mathfrak{g}_{-\alpha}$ component.*

For our purpose, we only need to establish its analogs for $\mathfrak{g}$ of type A_n and B_n.

Lemma 3.19. *Assume l is large enough for $\mathfrak{g}$. For $\mathfrak{g}$ of type A_n, there is a root $\alpha \in \Phi$ such that every irreducible submodule of $\bar{\rho}(\mathfrak{g})$ has a vector with nonzero $\mathfrak{l}_\alpha$ component and a vector with nonzero $\mathfrak{g}_{-\alpha}$ component.*

Proof. Let $\mathfrak{g} = \mathfrak{sl}_{n+1}$ and let $\alpha_{i,j} = e_i - e_j$, $i \neq j$ be the roots of $\mathfrak{g}$. Let $E_{i,j}$ be the $n+1$ by $n+1$ matrix that has 1 at the (i,j)-entry and zeros elsewhere. The $\mathfrak{sl}_2$-triple associated to $\alpha_{i,j}$ is $\{X_{i,j} := E_{i,j}, H_{i,j} = E_{i,i} - E_{j,j}, Y_{i,j} := E_{j,i}\}$. Let

$$X = X_{1,2} + X_{2,3} + \cdots + X_{n,n+1},$$

$$H = \sum_{i<j} H_{i,j} = k_1 H_{1,2} + k_2 H_{2,3} + \cdots + k_n H_{n,n+1},$$

$$Y = k_1 Y_{1,2} + k_2 Y_{2,3} + \cdots + k_n Y_{n,n+1},$$

where $k_i := i(n - i + 1)$. The triple $\{X, H, Y\}$ is an $\mathfrak{sl}_2$-triple containing the regular unipotent element X.

A straightforward calculation gives for $i < j$

$$[Y, X_{i,j}] = k_i X_{i+1,j} - k_{j-1} X_{i,j-1}.$$

Put $h = j - i$ and apply the above identity recursively, we obtain

$$(adY)^h X_{i,j} = (-1)^h k_{i,j} \left(H_{i,i+1} - \binom{h-1}{1} H_{i+1,i+2} + \binom{h-1}{2} H_{i+2,i+3} + \cdots + (-1)^{h-1} \binom{h-1}{h-1} H_{j-1} \right),$$

where $k_{i,j} = k_i k_{i+1} \cdots k_{j-1}$. By [Proposition 2.19](#),

$$\mathfrak{g}^X = \sum_{h=1}^{n} \langle v_{2h} \rangle$$

where $v_{2h} = \sum_{j-i=h} X_{i,j}$. Then we have

$$(adY)^h v_{2h} = h_1 H_{1,2} + \cdots + h_n H_{n,n+1}$$

with $h_1 = (-1)^h k_{1,h+1}$, $h_2 = (-1)^{h-1} \binom{h-1}{1} k_{1,h+1} + (-1)^h k_{2,h+2}$ and $h_i = (-1)^{h-1} h_{n-i+1}$. Since $(adY_{i,i+1}) H_{i-1,i} = Y_{i,i+1}$, $(adY_{i,i+1}) H_{i,i+1} = -2Y_{i,i+1}$ and $(adY_{i,i+1}) H_{i+1,i+2} = Y_{i,i+1}$,

$$(adY)^{h+1} v_{2h} = (adY)(h_1 H_{1,2} + \cdots + h_n H_{n,n+1})$$

$$= k_1(-2h_1 + h_2) Y_{1,2} + k_2(h_1 - 2h_2 + h_3) Y_{2,3} + \cdots + k_n(h_{n-1} - 2h_n) Y_{n,n+1}.$$

One computes

$$h_2 - 2h_1 = (-1)^{h-1}(h+1)! h(n-1)(n-2) \cdots (n-h+1) \neq 0.$$

So if we let $\alpha = \alpha_{1,2}$ and suppose l is large enough for $\mathfrak{g}$, then the submodule of $\bar{\rho}(\mathfrak{g})$ generated by v_{2h} has a vector with nonzero $\mathfrak{g}_{-\alpha}$ component, that is, the vector $(adY)^{h+1} v_{2h}$; the vector $(adY)^h v_{2h}$ has nonzero $\mathfrak{l}_\alpha$ component, as $\alpha(h_1 H_{1,2} + \cdots + h_n H_{n,n+1}) = 2h_1 - h_2$ which is nonzero. $\square$

Corollary 3.20. *Assume l is large enough for $\mathfrak{g}$. For $\mathfrak{g}$ of type B_n, there is a root $\alpha \in \Phi$ such that every irreducible submodule of $\bar{\rho}(\mathfrak{g})$ has a vector with nonzero $\mathfrak{l}_\alpha$ component and a vector with nonzero $\mathfrak{g}_{-\alpha}$ component.*

Proof. Let $\mathfrak{g} = \mathfrak{so}_{2n+1}$. Let $V = k^{2n+1}$ be a vector space equipped with a bilinear form $x_1 y_{2n+1} + x_2 y_{2n} + \cdots + x_{2n+1} y_1$ with matrix J. Then $\mathfrak{g}$ can be identified with

$$\{X \in M_{2n+1}(k) \mid XJ + JX^t = 0\}.$$

The roots of $\mathfrak{g}$ are $e_i - e_j$, $e_i + e_j$, $-e_i - e_j$, $\pm e_i$ for $1 \leq i \neq j \leq n$. We choose a set of simple roots $\Delta = \{e_1 - e_2, e_2 - e_3, \cdots e_{n-1} - e_n, e_n\}$. The $\mathfrak{sl}_2$-triple associated to $e_i - e_{i+1}$ is $\{X_i := X_{i,i+1} - X_{2n-i+1,2n-i+2}, H_i := H_{i,i+1} + H_{2n-i+1,2n-i+2}, Y_i := Y_{i,i+1} - Y_{2n-i+1,2n-i+2}\}$, and the $\mathfrak{sl}_2$-triple associated to e_n is $\{X_n := X_{n,n+1} - X_{n+1,n+2}, H_n := 2H_{n,n+1} + 2H_{n+1,n+2}, Y_n := 2Y_{n,n+1} - 2Y_{n+1,n+2}\}$. Let

$$X = \sum_i X_i,$$

$$H = \sum_{1 \leq i \leq n-1} i(2n - i + 1)H_i + \tfrac{1}{2}n(n+1)H_n,$$

$$Y = \sum_{1 \leq i \leq n-1} i(2n - i + 1)Y_i + \tfrac{1}{2}n(n+1)Y_n.$$

A straightforward calculation shows that X, H, Y form an $\mathfrak{sl}_2$-triple containing the regular unipotent element $X \in \mathfrak{g}$.

Corresponding to the exponents $1, 3, \cdots, 2n-1$ of $\mathfrak{g}$, we put

$$v_{2 \cdot 1} = X_{1,2} + \cdots + X_{n,n+1} - X_{n+1,n+2} - \cdots - X_{2n,2n+1} \in \mathfrak{so}_{2n+1},$$

$$v_{2 \cdot 3} = X_{1,4} + \cdots + X_{n-1,n+2} - X_{n,n+3} - \cdots - X_{2n-2,2n+1} \in \mathfrak{so}_{2n+1}, \ldots, \ldots,$$

$$v_{2 \cdot (2n-1)} = X_{1,2n} - X_{2,2n+1} \in \mathfrak{so}_{2n+1}.$$

Then $\mathfrak{g}^X = \sum_{i=1,3,\cdots,2n-1} < v_{2i} >$. Let $\alpha = e_1 - e_2$, the same calculation as in the proof of Lemma 3.19 gives $(adY)^i v_{2i}$ has a nonzero $\mathfrak{l}_\alpha$ component and $(adY)^{i+1} v_{2i}$ has a nonzero $\mathfrak{g}_{-\alpha}$ component for any exponent i. □

3D. *Removing the congruence conditions on l.* In this section, we use a result in [Fakhruddin et al. 2018] to remove the congruence condition we have imposed for G of type B_n, C_n, E_7 in Theorem 3.16. The following theorem is a simplified version of [Fakhruddin et al. 2018, Theorem 1.3]: as we are not considering geometric lifts, we relax the condition at l and only require the right hand side of Wiles' formula (Proposition 4.10) to be nonnegative. It applies to the residual representations we construct and allows us to deform it to an l-adic representation with Zariski-dense image for almost all primes l. However, their argument is very different and much more complicated than ours, so we only use it to remove the congruence conditions.

Theorem 3.21. *Suppose that there is a global deformation condition* $\mathcal{L} = \{L_v\}_{v \in S}$ *consisting of* smooth *local deformation conditions for each place* $v \in S$. *Let* $K = \mathbb{Q}(\bar{\rho}(\mathfrak{g}), \mu_l)$. *We assume the following*:

(1)
$$\sum_{v \in S} (\dim L_v) \geq \sum_{v \in S} h^0(\Gamma_{\mathbb{Q}_v}, \bar{\rho}(\mathfrak{g})).$$

(2) *The field* K *does not contain* μ_{l^2}.

(3) *The groups* $H^1(\mathrm{Gal}\,(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g}))$ *and* $H^1(\mathrm{Gal}\,(K/\mathbb{Q}), \bar{\rho}(\mathfrak{g})(1))$ *vanish.*

(4) *The spaces* $\bar{\rho}(\mathfrak{g})$ *and* $\bar{\rho}(\mathfrak{g})(1)$ *are semisimple* $\mathbb{F}_l[\Gamma_{\mathbb{Q}}]$-*modules (equivalently,* $k[\Gamma_{\mathbb{Q}}]$-*modules) having no common* $\mathbb{F}_l[\Gamma_{\mathbb{Q}}]$-*subquotient, and that neither contains the trivial representation.*

(5) *The space* $\bar{\rho}(\mathfrak{g})$ *is multiplicity-free as a* $\mathbb{F}_l[\Gamma_{\mathbb{Q}}]$-*module.*

Then there exists a finite set of primes Q *disjoint from* S, *and a lift* $\rho : \Gamma_{\mathbb{Q}, S \cup Q} \to G(\mathcal{O})$ *of* $\bar{\rho}$ *such that* ρ *is of type* L_v *at all* $v \in S$.

Lemma 3.22. *Let* $k = \mathbb{F}_l$ *and let* $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ *be as in Sections 2A4–2A6. Then Theorem 3.21(2)–(5) hold.*

Proof. By the decomposition of $\bar{\rho}(\mathfrak{g})$ and the proof of Proposition 3.5(3)–(5) hold. It remains to show (2). Since by construction $\bar{\rho}$ is unramified at l, $\mathbb{Q}(\bar{\rho}(\mathfrak{g}))$ and $\mathbb{Q}(\mu_l)$ are linearly disjoint over $\mathbb{Q}$. It follows that

$$\mathrm{Gal}\,(K/\mathbb{Q}) \cong (\mathrm{Im}(\bar{\rho})/Z) \times (\mathbb{Z}/l\mathbb{Z})^{\times}$$

where Z denotes the center of $G(k)$. Assume K contains μ_{l^2}, then there would be a surjection

$$\mathrm{Gal}\,(K/\mathbb{Q})^{\mathrm{ab}} \twoheadrightarrow (\mathbb{Z}/l^2\mathbb{Z})^{\times}.$$

On the other hand, we have by the construction of $\bar{\rho}$ that $\mathrm{Im}(\bar{\rho})' = \mathrm{Im}(\bar{\rho})$ for G of type B_n and E_7, $\mathrm{Im}(\bar{\rho})'$ is of index two in $\mathrm{Im}(\bar{\rho})$ for G of type C_n. It follows that the order of $(\mathrm{Im}(\bar{\rho})/Z)^{\mathrm{ab}}$ is at most two, and hence the order of $\mathrm{Gal}\,(K/\mathbb{Q})^{\mathrm{ab}}$ is at most $2(l-1)$. But this is impossible since $(\mathbb{Z}/l^2\mathbb{Z})^{\times}$ has order $l(l-1)$ and $l \neq 2$. $\qquad\square$

4. Simple, simply connected groups as monodromy groups

In this section, we prove Theorem 1.2 for G a simple, simply connected algebraic group. Recall that there are two different constructions for the residual representation $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$: one has image a large index subgroup of $N_G(T)_k$ with the properties that $\bar{\rho}$ is unramified at l and $\mathrm{ad}\,\bar{\rho}(c)$ is nontrivial; the other factors through a principal GL_2 such that $\bar{\rho}(c) = \rho^{\vee}(-1)$.

4A. *Local deformation conditions.* We need to define several local deformation conditions for deforming the mod p representations.

4A1. *The archimedean place.* Recall that in Sections 2A3–2A5, we construct the residual representations by first realizing S_n or A_n as a Galois group over $\mathbb{Q}$ and then repeatedly applying Theorem 2.5 to build the Galois extension realizing N or a subgroup of it over $\mathbb{Q}$. We write c for the nontrivial element in $\Gamma_{\mathbb{R}}$, the complex conjugation.

Proposition 4.1. *Let G be of classical type and $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ be as in Sections 2A2-2A5. In particular, $\mathrm{ad}\,\bar{\rho}(c)$ is nontrivial. Then:*

(1) *For G of type A_{n-1}, $h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{g})) \leq n^2 - 2n + 1$.*

(2) *For G of type B_n, $h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{g})) \leq 2n^2 - 3n + 2$.*

(3) *For G of type C_n, $h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{g})) \leq 2n^2 - 3n + 4$.*

(4) *For G of type D_n, $h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{g})) \leq 2n^2 - 5n + 4$.*

Proof. Let f be the number of root vectors that are fixed by $\bar{\rho}(c)$. Let us recall that $\mathrm{ad}\,\bar{\rho}(c)$ is nontrivial by Theorem 2.4.

If G is of type A_{n-1}, we have $G(k) \cong \mathrm{SL}(V)$ with $V = k^n$. Let $d := \dim V^{\bar{\rho}(c)}$. Then

$$f = 2\left(\binom{d}{2} + \binom{n-d}{2} \right).$$

If G is of type B_n, $G(k)/\mu_2 \cong \mathrm{SO}(V)$ with $V = k^{2n+1}$ a k-vector space equipped with the nondegenerate symmetric bilinear form $x_1 y_{2n+1} + x_2 y_{2n} + \cdots + x_{2n+1} y_1$. We may assume $\bar{\rho}(c)$ is conjugate to $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n, 1, \epsilon_n, \ldots, \epsilon_1)$ in $\mathrm{SO}(V)$ and let d be the number of ones among $\epsilon_1, \ldots, \epsilon_n$. Then

$$f = 4\left(\binom{d}{2} + \binom{n-d}{2} \right) + 2d.$$

If G is of type C_n, $G(k) \cong \mathrm{Sp}(V)$ with $V = k^{2n}$ a k-vector space equipped with the nondegenerate alternating bilinear form $x_1 y_{2n} + \cdots x_n y_{n+1} - x_{n+1} y_n - \cdots - x_{2n} y_1$. We may assume $\bar{\rho}(c)$ is conjugate to $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n, \epsilon_n, \ldots, \epsilon_1)$ and let d be the number of 1's among $\epsilon_1, \ldots, \epsilon_n$. Then

$$f = 4\left(\binom{d}{2} + \binom{n-d}{2} \right) + 2n.$$

If G is of type D_n, a quotient of $G(k)$ is isomorphic to $\mathrm{SO}(V)$ with $V = k^{2n}$ a k-vector space equipped with the nondegenerate symmetric bilinear form $x_1 y_{2n} + x_2 y_{2n-1} + \cdots + x_{2n} y_1$. We may assume $\bar{\rho}(c)$ is conjugate to $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n, \epsilon_n, \ldots, \epsilon_1)$ in $\mathrm{SO}(V)$ and let d be the number of 1's among $\epsilon_1, \ldots, \epsilon_n$. Then

$$f = 4\left(\binom{d}{2} + \binom{n-d}{2} \right).$$

By the construction of $\bar{\rho}$ (see the paragraph before Remark 2.8 in Section 2A3 for type A_n; for other types, see Sections 2A4, 2A5 and 2A6), $\mathrm{ad}\,\bar{\rho}(c)$ is nontrivial, which implies $0 < d < n$. So f attains its maximum when $d = n - 1$. Since

$$h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{g})) = rk(\mathfrak{g}) + f,$$

the upper bounds can then be computed easily.   □

Proposition 4.2. *Let G be of type E_7 and $\bar{\rho} : \Gamma_\mathbb{Q} \to G(k)$ be as in [Section 2A6](). In particular*, ad $\bar{\rho}(c)$ *is nontrivial. Then* $h^0(\Gamma_\mathbb{R}, \bar{\rho}(\mathfrak{g})) \leq 7 + 126 - 14 = 119$.

Proof. Suppose that $\bar{\rho}(c) \in T(k)$ for a maximal torus T split over k. Let $\Phi = \Phi(G, T)$, and $\mathfrak{g}_\Phi = \sum_{\alpha \in \Phi} \mathfrak{g}_\alpha$ be the k-subspace of $\bar{\rho}(\mathfrak{g})$ generated by all root vectors. The Lie algebra $\mathfrak{t}$ of $T(k)$, which has k-dimension 7, is clearly fixed by ad $\bar{\rho}(c)$. Thus, it suffices to show that the -1-eigenspace of ad $\bar{\rho}(c) \mid \mathfrak{g}_\Phi$ has k-dimension at least 14. We consider ad $\bar{\rho}(c) \mid \mathfrak{g}_{\Phi'}$ where $\Phi' \subset \Phi$ is of type A_7. This action is nontrivial. By the A_n-calculation in the proof of [Proposition 4.1]() (letting $n = 7$), the -1-eigenspace of ad $\bar{\rho}(c) \mid \mathfrak{g}_{\Phi'}$ has dimension at least twice the rank of Φ', proves the proposition.   □

The following lemma is clear.

Lemma 4.3. *The dimension*

$$\dim_k (\mathrm{Sym}^{2n}(k^2) \otimes \det^{-n})^{\mathrm{diag}(1,-1)}$$

equals n when n is odd, and $n + 1$ when n is even.

Corollary 4.4. *Let $\bar{\rho} : \Gamma_\mathbb{Q} \to G(k)$ be as in [Section 2B](). Then*

$$h^0(\Gamma_\mathbb{R}, \bar{\rho}(\mathfrak{g})) = 4 \qquad \textit{for } G = \mathrm{SL}_3,$$
$$h^0(\Gamma_\mathbb{R}, \bar{\rho}(\mathfrak{g})) = 9 \qquad \textit{for } G = \mathrm{Spin}_7,$$
$$h^0(\Gamma_\mathbb{R}, \bar{\rho}(\mathfrak{g})) = 38 \quad \textit{for } G = E_6^{\mathrm{sc}}.$$

Proof. This follows from [Lemma 4.3]() and [Proposition 2.19](). Note that the complex conjugation maps to $\mathrm{diag}(1, -1)$ in GL_2 because the representation $r_{f,\lambda}$ in the last paragraph of [Section 2]() is odd.   □

4A2. *The place l.* As we are not looking for geometric l-adic Galois representations in this paper, we impose *no condition* at the place l. So the tangent space is $H^1(\Gamma_l, \bar{\rho}(\mathfrak{g}))$. By the local Euler characteristic formula,

$$h^1(\Gamma_l, \bar{\rho}(\mathfrak{g})) = h^0(\Gamma_l, \bar{\rho}(\mathfrak{g})) + h^2(\Gamma_l, \bar{\rho}(\mathfrak{g})) + \dim_k \mathfrak{g}.$$

Lemma 4.5. *Let $\bar{\rho}$ be as in [Section 2A or 2B](). Then $h^2(\Gamma_l, \bar{\rho}(\mathfrak{g})) = 0$ for large enough primes l.*

Proof. By local duality, it suffices to show that $h^0(\Gamma_l, \bar{\rho}(\mathfrak{g})(1)) = 0$. For the representation $\bar{\rho}$ in [Section 2A](), $\bar{\rho}(I_{\mathbb{Q}_l})$ is trivial by construction but $\bar{\kappa}(I_{\mathbb{Q}_l})$ is nontrivial, so $\bar{\rho}(\mathfrak{g})(1)^{I_{\mathbb{Q}_v}}$ is trivial. In particular, $h^0(\Gamma_l, \bar{\rho}(\mathfrak{g})(1)) = 0$. For the representation $\bar{\rho}$ in [Section 2B](), [Proposition 2.19]() and the lemma below imply $h^0(\Gamma_l, \bar{\rho}(\mathfrak{g})(1)) = 0$.   □

Lemma 4.6. *We have $h^0(\Gamma_l, \mathrm{Sym}^{2m}(\bar{r}_f) \otimes \det(\bar{r}_f)^{-m} \otimes \bar{\kappa}) = 0$ for $m \geq 1$ and large enough primes l (relative to m).*

Proof. The argument is similar to the proof of [Weston 2004, Proposition 4.4]. Let K be a finite extension of $\mathbb{Q}_l$ with ring of integers $\mathcal{O}$ and residue field k. Let $v : K^\times \to \mathbb{Q}$ be the valuation on K, normalized so that $v(l) = 1$. We briefly recall the setting in Section 4.1 of [Weston 2004]. For $a < b$, let $\mathcal{MF}^{a,b}(\mathcal{O})$ denote

the category of filtered Dieudonné $\mathcal{O}$-modules D equipped with a decreasing filtration of $\mathcal{O}$-modules $\{D_i\}_{i \in \mathbb{Z}}$ and a family of $\mathcal{O}$-linear maps $\{f_i : D^i \to D\}$ satisfying $D^a = D$ and $D^b = 0$; see [Weston 2004, Definition 4.1]. Let $\mathcal{G}^{a,b}(\mathcal{O})$ denote the category of finite type $\mathcal{O}$-module subquotients of crystalline K-representations V with $D^a_{\mathrm{crys}}(V) = D_{\mathrm{crys}}(V)$ and $D^b_{\mathrm{crys}}(V) = 0$. Fontaine–Laffaille define a functor

$$\mathcal{U} : \mathcal{MF}^{a,a+l}(\mathcal{O}) \to \mathcal{G}^{a,a+l}(\mathcal{O})$$

satisfying a list of properties including $\mathcal{U}$ that is stable under formation of subobjects and quotients, and compatible with tensor products for l large enough. In particular, $\mathcal{U}$ is compatible with symmetric powers for large enough l. Let $\varepsilon : \Gamma_l \to \mathcal{O}^\times$ be an unramified character of finite order and let $\mathcal{O}(\varepsilon)$ denote a free $\mathcal{O}$-module of rank 1 with Γ_l-action via ε. Then $\mathcal{O}(\varepsilon) \in \mathcal{G}^{0,1}(\mathcal{O})$, so that there is $D_\varepsilon \in \mathcal{MF}^{0,1}(\mathcal{O})$ such that $\mathcal{U}(D_\varepsilon) = \mathcal{O}(\varepsilon)$. This D_ε is a free $\mathcal{O}$-module of rank one with $D_\varepsilon = D^0_\varepsilon$ and $f_0 : D^0_\varepsilon \to D_\varepsilon$ the multiplication by $\varepsilon^{-1}(l) := \varepsilon^{-1}(\mathrm{Fr}_l)$ where the Frobenius element is arithmetic.

Let f be a newform of weight 3, level N, and character ε. Let $K \supset E_\lambda$ and let $r_f := r_{f,\lambda} : \Gamma_\mathbb{Q} \to \mathrm{GL}_2(K)$ be the Galois representation associated to f of weight k (see Example 1.5). We fix an embedding $\Gamma_l \to \Gamma_\mathbb{Q}$, and let V_f be a two dimensional K-vector space on which Γ_l acts via $r_f \mid \Gamma_l$, and fix a Γ_l-stable $\mathcal{O}$-lattice $T_f \subset V_f$. If l does not divide N, then V_f is crystalline and $T_f \in \mathcal{G}^{0,3}(\mathcal{O})$. Thus for $l > k$ there exists $D_f \in \mathcal{MF}^{0,3}(\mathcal{O})$ with $\mathcal{U}(D_f) \cong T_f$. The filtration on D_f satisfies $\mathrm{rk}_\mathcal{O}(D^i_f) = 2$ if $i \leq 0$, $\mathrm{rk}_\mathcal{O}(D^i_f) = 1$ if $1 \leq i \leq 2$, and $\mathrm{rk}_\mathcal{O}(D^i_f) = 0$ if $i \geq 3$. Choose an $\mathcal{O}$-basis x, y of D_f with x an $\mathcal{O}$-generator of D^1_f. Let $a, b, c, d \in \mathcal{O}$ be such that $f_0 x = ax + by$, $f_0 y = cx + dy$. Then $a + d = a_l$ and $ad - bc = l^2 \varepsilon(l)$. We have $v(a), v(b) \geq 2$.

Let $\bar{r}_f : \Gamma_l \to \mathrm{GL}_2(k)$ be the Galois representation $T_f / \lambda T_f$. Since $\det r_f = \kappa^2 \varepsilon$, we have

$$\mathrm{Sym}^{2m}(T_f) \otimes \det(T_f)^{-m} \otimes \kappa = (\mathrm{Sym}^{2m}(T_f) \otimes \mathcal{O}(\varepsilon^{-m}))(1 - 2m).$$

When l is large enough relative to m, by [Fontaine and Messing 1987, Proposition 1.7] we can take

$$D = (\mathrm{Sym}^{2m}(D_f) \otimes D_{\varepsilon^{-m}})(2m - 1).$$

Further, since $(\mathrm{Sym}^{2m}(T_f) \otimes \det(T_f)^{-m} \otimes \kappa)/\lambda$ is a realization of $\mathrm{Sym}^{2m}(\bar{r}_f) \otimes \det(\bar{r}_f)^{-m} \otimes \bar{\kappa}$, we have

$$H^0(\Gamma_l, \mathrm{Sym}^{2m}(\bar{r}_f) \otimes \det(\bar{r}_f)^{-m} \otimes \bar{\kappa}) = \ker(1 - f_0 : D^0/\lambda D^0 \to D/\lambda D).$$

By the definition of Tate twists and tensor products of filtered Dieudonné $\mathcal{O}$-modules, we have

$$D^0 = (\mathrm{Sym}^{2m}(D_f) \otimes D_{\varepsilon^{-m}})^{2m-1} = \sum_{i_1 + \cdots + i_{2m} + j = 2m-1} D^{i_1}_f \cdots D^{i_{2m}}_f \cdot D^j_{\varepsilon^{-m}} = \sum_{i_1 + \cdots + i_{2m} = 2m-1} D^{i_1}_f \cdots D^{i_{2m}}_f \cdot D^0_{\varepsilon^{-m}}.$$

To make the sum nonzero, there must be at least m indices that are greater than or equal to 1, so at least m indices must be two since $x \in D^2_f$ as well as D^1_f. It follows that $\{x^i y^{2m-i-1} w \mid i \geq m\}$ is an $\mathcal{O}$-basis of D^0, where w is an $\mathcal{O}$-generator of $D_{\varepsilon^{-m}}$. We compute

$$f_0(x^i y^{2m-i-1} w) = \frac{\varepsilon^m(l)}{l^{2m-1}} (ax + by)^i (cx + dy)^{2m-i-1}.$$

Since $v(a), v(b) \geq 2$ and $i \geq m$, all the coefficients of x and y have positive valuations. Therefore, $f_0(x^i y^{2m-i-1} w) \equiv 0$ modulo λ, which implies $f_0 : D^0/\lambda D^0 \to D/\lambda D$ is zero. It follows that $H^0(\Gamma_l, \mathrm{Sym}^{2m}(\bar{r}_f) \otimes \det(\bar{r}_f)^{-m} \otimes \bar{\kappa})$ is trivial. $\qquad\square$

Corollary 4.7. $h^1(\Gamma_l, \bar{\rho}(\mathfrak{g})) = h^0(\Gamma_l, \bar{\rho}(\mathfrak{g})) + \dim_k \mathfrak{g}$.

4A3. *A zero-dimensional deformation.* In order to maximize the Zariski-closure of the image of the l-adic lift of the residual representation, we need to impose a simple local deformation condition at some unramified place.

Suppose that $p \neq l$, F is a finite extension of $\mathbb{Q}_p$, and $\bar{\rho} : \Gamma_F \to G(k)$ is an unramified representation. Let $g \in G(\mathcal{O})$ be a lift of $\bar{\rho}(\mathrm{Fr}_p)$.

Definition 4.8. Define

$$\mathrm{Lift}^g_{\bar{\rho}} : \mathrm{CNL}_{\mathcal{O}} \to \mathbf{Sets}$$

such that for a complete local noetherian $\mathcal{O}$-algebra R, $\mathrm{Lift}^g_{\bar{\rho}}(R)$ consists of all lifts

$$\rho : \Gamma_F \to G(R)$$

of $\bar{\rho}$ such that ρ is unramified and $\rho(\mathrm{Fr}_p)$ is $\hat{G}(R)$-conjugate to g.

So the tangent space is zero-dimensional and when $\mathrm{Lift}^g_{\bar{\rho}}$ is a local deformation condition, it is clearly smooth. But for a given g, $\mathrm{Lift}^g_{\bar{\rho}}$ may not be representable. But at least we have

Proposition 4.9. *Suppose that G is simply connected. Let $\bar{g}$ and g be regular semisimple elements of $G(\bar{\mathbb{F}}_l)$ and $G(\bar{\mathbb{Q}}_l)$, respectively. Then $\mathrm{Lift}^g_{\bar{\rho}}$ is representable.*

Proof. By Schlessinger's criterion, it suffices to show the following: for any $A \twoheadrightarrow B$ in $\mathrm{CLN}_{\mathcal{O}}$ with kernel I for which $I \cdot \mathfrak{m}_A = 0$, the induced map

$$Z_G(g)(A) \to Z_G(g)(B)$$

is surjective. The group $Z_G(g)$ is a scheme over $\mathcal{O}$, we denote the structure map by

$$f : Z_G(g) \to \mathrm{Spec}\,\mathcal{O}.$$

We need to show that $Z_G(g)$ is a smooth $\mathcal{O}$-scheme. It suffices to show that:

- The map f is flat over $\mathcal{O}$.
- The generic fiber and the special fiber of f are smooth of the same dimension.

Because G is simply connected and $\bar{g}$ and g are regular semisimple, $Z_G(g)(\mathcal{O}/\lambda)$ and $Z_G(g)(\mathrm{Frac}\,\mathcal{O})$ are connected maximal tori of $G(\mathcal{O}/\lambda)$ and $G(\mathrm{Frac}\,\mathcal{O})$, respectively, with dimension the rank of G. The second bullet follows.

To show the first bullet, note that f has a section, that is, $Z_G(g)$ has an $\mathcal{O}$-point (for example, the element $g \in G(\mathcal{O})$ itself). Moreover, by the previous paragraph, the generic fiber and the special fiber of f are both irreducible, reduced and have the same dimension. It follows from Proposition 6.1 of [Gan and Yu 2003] that f is flat. $\qquad\square$

4A4. *Steinberg deformations.* In [Patrikis 2016, Section 4.3], a local deformation condition of "Steinberg type" is taken at a place in order to obtain a regular unipotent element in the image of the l-adic lift. *We will only need this in deforming those $\bar{\rho}$ constructed from the principal* GL_2. We refer the reader to [Patrikis 2016, Section 4.3] for the definition and properties of the Steinberg deformation condition. The dimension of the tangent space equals $h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}))$.

4A5. *Minimal prime to l deformations.* This deformation condition is well known; see [Patrikis 2016, Section 4.4] for its definition. We will use this deformation condition at places $v \neq l$ for which $\bar{\rho}(I_{\mathbb{Q}_v})$ is nontrivial and $\bar{\rho}(\Gamma_{\mathbb{Q}_v})$ has order prime to l. The tangent space is $H^1(\Gamma_v/I_v, \bar{\rho}(\mathfrak{g})^{I_v})$, whose dimension is $h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}))$.

4B. ***Deforming* mod *p Galois representations.*** In this section, we specify the global deformation condition and compute the Wiles formula, then use the results in Section 3 to prove Theorem 1.2. Let us recall Wiles' formula, for a proof; see [Patrikis 2016, Proposition 9.2].

Proposition 4.10. *Let M be a finite-dimensional k-vector space with a continuous $\Gamma_{\mathbb{Q}}$ action unramified outside a finite set of places S. Let $\mathcal{L} = \{L_v\}_{v \in S}$ and $\mathcal{L}^\perp = \{L_v^\perp\}_{v \in S}$ be a Selmer system and dual Selmer system, respectively, for M. Then*

$$h^1_{\mathcal{L}}(\Gamma_S, M) - h^1_{\mathcal{L}^\perp}(\Gamma_S, M^\vee) = h^0(\Gamma_S, M) - h^0(\Gamma_S, M^\vee) + \sum_{v \in S}(\dim_k L_v - h^0(\Gamma_v, M)).$$

We will compute the right-hand side of the identity for $M = \bar{\rho}(\mathfrak{g})$ or $\bar{\rho}(\mathfrak{t})$ and for a global deformation condition to be specified below. For $\bar{\rho}(\mathfrak{g})$ from either Section 2A or 2B, note that $h^0(\Gamma_S, \bar{\rho}(\mathfrak{g})) = h^0(\Gamma_S, \bar{\rho}(\mathfrak{g})(1)) = 0$.

4B1. *Weyl group case.* For G a simple, simply connected group of classical type or type E_7, let $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ be as in Section 2A. Here we exclude the A_1, A_2, B_3 cases. We impose no condition at $v = l$ which is liftable by Lemma 4.5, and impose the minimal prime to l condition at $v \in S - \{\infty, l\}$ (note that $\bar{\rho}(\Gamma_{\mathbb{Q}})$ has order prime to l by our construction). Moreover, we will find a prime $p \notin S$ for which $\bar{\rho}(\mathrm{Fr}_p)$ is regular semisimple, together with a regular semisimple lift $g \in G(\mathcal{O})$ of $\bar{\rho}(\mathrm{Fr}_p)$. Then we take the deformation condition $\mathrm{Lift}^g_{\bar{\rho}|_{\Gamma_p}}$ at p.

Lemma 4.11.
$$\sum_{v \in S} \dim_k L_v \geq \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g})).$$

Proof. This follows directly the local computations in Section 4A, for example Proposition 4.1 and Corollary 4.7, etc. We record here a lower bound for $\sum_{v \in S} \dim_k L_v - \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{g}))$. For $G = \mathrm{SL}_n$, it is $n - 1$; for $G = \mathrm{Spin}_{2n+1}$, it is $3n - 2$; for $G = \mathrm{Sp}_{2n}$, it is $3n - 4$; for $G = \mathrm{Spin}_{2n}$, it is $3n - 4$; and for $G = E_7$, it is 7. $\qquad\square$

Lemma 4.12.
$$\sum_{v \in S} \dim_k(L_v \cap H^1(\Gamma_v, \bar{\rho}(\mathfrak{t}))) \leq \sum_{v \in S} h^0(\Gamma_v, \bar{\rho}(\mathfrak{t})).$$

Proof. For $v \notin \{\infty, l, p\}$, L_v corresponds to the minimal prime to l deformation condition and we have

$$\dim_k(L_v \cap H^1(\Gamma_v, \bar{\rho}(\mathfrak{t}))) = \dim_k H^1(\Gamma_v/I_v, \bar{\rho}(\mathfrak{t})^{I_v}) = h^0(\Gamma_v, \bar{\rho}(\mathfrak{t})).$$

So it suffices to compare both sides for $v \in \{\infty, l, p\}$. The left-hand side subtracting the right-hand side equals

$$(0 - h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{t}))) + (h^1(\Gamma_l, \bar{\rho}(\mathfrak{t})) - h^0(\Gamma_l, \bar{\rho}(\mathfrak{t}))) + (0 - h^0(\Gamma_p, \bar{\rho}(\mathfrak{t}))).$$

By local duality and Lemma 4.5,

$$h^1(\Gamma_l, \bar{\rho}(\mathfrak{t})) - h^0(\Gamma_l, \bar{\rho}(\mathfrak{t})) = \dim_k \mathfrak{t}.$$

Combining this with the identity

$$h^0(\Gamma_p, \bar{\rho}(\mathfrak{t})) = \dim_k \mathfrak{t},$$

we see that the difference is $-h^0(\Gamma_{\mathbb{R}}, \bar{\rho}(\mathfrak{t})) \leq 0$. ☐

Let us make the following observation which is from [Patrikis 2016, Lemma 7.7]. It will be used frequently in the proof of Propositions 4.14, 4.18, and 4.20; suppose that $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ is a continuous representation with a continuous lift $\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$. Let G_ρ be the Zariski closure of $G(\mathcal{O})$ in $G(\bar{\mathbb{Q}}_l)$. Then $\mathrm{Lie}(G_\rho)$, $\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_{\mathcal{O}}$, and $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_{\mathcal{O}}) \otimes_{\mathcal{O}} k$ are $\Gamma_{\mathbb{Q}}$-modules. Moreover, the last one is a submodule of $\bar{\rho}(\mathfrak{g})$ and thus is a direct sum of some irreducible summands of $\bar{\rho}(\mathfrak{g})$. If $\mathrm{Lie}(G_\rho) = \mathfrak{g}(\bar{\mathbb{Q}}_l)$ (which is equivalent to $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_{\mathcal{O}}) \otimes_{\mathcal{O}} k = \mathfrak{g}$), then $G_\rho = G(\bar{\mathbb{Q}}_l)$ (since G is connected).

Lemma 4.13. *Let G be a semisimple algebraic group defined over $\mathcal{O}$ and let C be a proper subvariety of G. Let $g \in G(\mathcal{O})$ and $H = g\hat{G}(\mathcal{O})$ be the corresponding $\hat{G}(\mathcal{O})$-coset of $G(\mathcal{O})$. Then there is a regular semisimple element in $H - C(\bar{\mathbb{Q}}_l)$.*

Proof. Let V be the union of $C(\bar{\mathbb{Q}}_l)$ and the set of elements of $G(\bar{\mathbb{Q}}_l)$ that are not regular semisimple. Then V is a proper Zariski-closed subset of $G(\bar{\mathbb{Q}}_l)$ as the set of regular semisimple elements is Zariski-open (see for example [Humphreys 1995, Theorem 2.5]). On the other hand, H is Zariski-dense in $G(\bar{\mathbb{Q}}_l)$. If there were no regular semisimple element in $H - C(\bar{\mathbb{Q}}_l)$, then $H \subset V$ and H could not be Zariski-dense, a contradiction. ☐

Proposition 4.14. *Let G be a simple, simply connected group of classical type (excluding type A_1, A_2 and B_3) or type E_7. Then for almost all primes l when Φ is of type A_n or D_n, for almost all primes $l \equiv 1(4)$ when Φ is of type B_n or C_n, and for almost all primes $l \equiv 1(3)$ when Φ is of type E_7, there are l-adic lifts*

$$\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$$

of $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ defined in Section 2A with Zariski-dense image in $G(\bar{\mathbb{Q}}_l)$.

Proof. By Lemmas 4.11 and 4.12, we can apply Theorem 3.16 to obtain a lift $\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$ satisfying the prescribed local conditions. The condition at p implies that G_ρ has infinitely many elements and so $\mathrm{Lie}(G_\rho)$ is nontrivial.

If G is of type A_n or D_n, by Propositions 2.9 and 2.13, $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ (as a Lie subalgebra of $\mathfrak{g}$) is then either $\mathfrak{t}$ or $\mathfrak{g}$. By the previous lemma, there exist a regular semisimple element $g \in G(\mathcal{O})$ such that $\bar{g} = \bar{\rho}(\mathrm{Fr}_p)$ and $g \notin N_G(T)(\overline{\mathbb{Q}}_l)$. Imposing $\mathrm{Lift}^g_{\bar{\rho}\,|\,p}$ at p, we obtain $G_\rho \not\subseteq N_G(T)(\overline{\mathbb{Q}}_l)$, which implies $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ cannot be $\mathfrak{t}$.

If G is of type B_n, by Proposition 2.13, $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ (as a Lie subalgebra of $\mathfrak{g}$) is $\mathfrak{t}$, $\mathfrak{t} \oplus \mathfrak{g}_l \cong \mathfrak{so}_{2n}$ or $\mathfrak{g}$. Let H be an algebraic subgroup of G containing T such that $(\mathrm{Lie}(H) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k = \mathfrak{t} \oplus \mathfrak{g}_l$ (there are finitely many of them). Let C be the union of $N_G(T)$ and all such H, which is a proper subvariety of G. By the previous lemma, there exist a regular semisimple element $g \in G(\mathcal{O})$ such that $\bar{g} = \bar{\rho}(\mathrm{Fr}_p)$ and $g \notin C(\overline{\mathbb{Q}}_l)$. Imposing $\mathrm{Lift}^g_{\bar{\rho}\,|\,p}$ at p, we obtain $G_\rho \not\subseteq C(\overline{\mathbb{Q}}_l)$, which implies $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ cannot be $\mathfrak{t}$ or $\mathfrak{t} \oplus \mathfrak{g}_l$.

If G is of type C_n, by Proposition 2.11, $(Lie(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ (as a Lie subalgebra of $\mathfrak{g}$) is $\mathfrak{t}$, $\mathfrak{t} \oplus \mathfrak{g}_l \cong (\mathfrak{sl}_2)^n$ or $\mathfrak{g}$. The same argument as for type B_n enables us to impose a suitable condition $\mathrm{Lift}^g_{\bar{\rho}\,|\,p}$ at p in order to force $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k = \mathfrak{g}$.

Finally, suppose that $G = E_7^{\mathrm{sc}}$. By Proposition 2.17, $(Lie(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ (as a Lie subalgebra of $\mathfrak{g}$) is either $\mathfrak{t}$, $\mathfrak{t} \oplus \mathfrak{g}_a \cong \mathfrak{sl}_7$ or $\mathfrak{g}$. We can force $(\mathrm{Lie}(G_\rho) \cap \mathfrak{g}_\mathcal{O}) \otimes_\mathcal{O} k$ to be $\mathfrak{g}$ in the same way as above. $\qquad\square$

Remark 4.15. As we have flexibilities in choosing $g \in G(\mathcal{O})$ lifting $\bar{\rho}(\mathrm{Fr}_p)$, it is easy to see that there are infinitely many lifts ρ that are nonconjugate in G^{ad}.

4B2. *Principal* GL_2 *case.* For G a simply connected group of one of the following types: A_2, B_3, E_6, let $\bar{\rho} : \Gamma_\mathbb{Q} \to G(k)$ be as in Section 2B.

We begin with the following proposition due to Tom Weston [2004, Proposition 5.3].

Proposition 4.16. *Let $\pi = \pi_f$ be a cuspidal automorphic representation corresponding to a holomorphic eigenform f of weight at least 2. Assume that for some prime p, π_p is isomorphic to a twist of the Steinberg representation of $\mathrm{GL}_2(\mathbb{Q}_p)$. Then for almost all λ, the local Galois representation $\bar{r}_{f,\lambda}|_{\Gamma_p}$ (in the notation of Example 1.5) has the form*

$$\bar{r}_{f,\lambda}|_{\Gamma_p} \sim \begin{pmatrix} \chi\bar{\kappa} & * \\ 0 & \chi \end{pmatrix}$$

where the extension $*$ in $H^1(\Gamma_p, k_\lambda(\bar{\kappa}))$ is nonzero.

Let f be a non-CM weight 3 cuspidal eigenform that is a newform of level $\Gamma_1(p) \cap \Gamma_0(q)$ for some primes p and q; the nebentypus of f is a character $\varepsilon : (\mathbb{Z}/pq\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$. Such a form f exists, see for example, [LMFDB 2013, 15.3.7.a and 15.3.11.a]. Note that the automorphic representation π_f associated to f is Steinberg at p. Proposition 4.16 together with the definition of principal GL_2 then imply $\bar{\rho}|_{\Gamma_p}$ is Steinberg in the sense of [Patrikis 2016, Definition 4.13]. At p we take the Steinberg deformation condition. As π_f is a principal series at q, $\bar{\rho}(I_q)$ has order prime to l. We then use the minimal prime to l deformation condition at q. At l we impose no condition. Moreover, choose an element $\sigma \in \Gamma_\mathbb{Q}$ such that $\bar{\rho}(\sigma)$ is regular semisimple in $T(k)$ together with a lift $g \in T(\mathcal{O})$ such that $\alpha(g)$,

$\alpha \in \Delta$ are distinct. By Chebotarev's density theorem, there is a prime $r \notin \{\infty, l, p, q\}$ such that $\mathrm{Fr}_r = \sigma$. We then take $\mathrm{Lift}_{\bar{\rho}|_{\Gamma_r}}^g$ at r. Let $\mathcal{L}$ be the Selmer system associated to the above local deformations.

Lemma 4.17. *The right-hand side of Wiles' formula is* 2 *for* A_2, 9 *for* B_3, *and* 34 *for* E_6.

Proof. This follows from Corollaries 4.4, 4.7 and Proposition 4.10. $\qquad\square$

Proposition 4.18. *For* $G = \mathrm{SL}_3$, Spin_7 *or* E_6^{sc} *and for almost all primes* l, *there are* l-*adic lifts*

$$\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$$

of $\bar{\rho} : \Gamma_{\mathbb{Q}} \to G(k)$ *defined as in Section 2B with Zariski-dense image in* $G(\bar{\mathbb{Q}}_l)$.

Proof. The proof is very similar to the proof of [Patrikis 2016, Theorem 7.4], so we skip a few details here.

We first show that Theorem 3.4 applies to $\bar{\rho}$. Item (1) is satisfied by Lemma 4.17; items (2) and (3) are satisfied by the proof of [Patrikis 2016, Theorem 7.4]; for item (4), take $\sigma \in \Gamma_{\mathbb{Q}}$ such that $\bar{\rho}(\sigma) = 2\rho^{\vee}(a)$ is regular with $1 \neq a \in (\mathbb{Z}/l\mathbb{Z})^{\times}$ and $\bar{\kappa}(\sigma) = a^2$ (which is possible, again, see the proof of [Patrikis 2016, Theorem 7.4]). It follows that item (a) is satisfied for any simple root α. Item (b) and (c) are also satisfied by Lemmas 3.18, 3.19 and Corollary 3.20.

Therefore, we can deform $\bar{\rho}$ to a continuous representation $\rho : \Gamma_{\mathbb{Q}} \to G(\mathcal{O})$ satisfying the prescribed local conditions on S and the Ramakrishna condition on a set of auxiliary primes disjoint from S. We write G_ρ for the Zariski closure of the image of ρ in $G(\bar{\mathbb{Q}}_l)$. By [Patrikis 2016, Lemma 7.7] G_ρ is reductive. By Proposition 4.16, the Steinberg condition at p ensures that G_ρ contains a regular unipotent element (see the proof of [Patrikis 2016, Theorem 8.4]). By a theorem of Dynkin [Saxl and Seitz 1997, Theorem A], G_ρ is then of type A_1 or A_2 for $G = \mathrm{SL}_3$, type A_1, G_2 or B_3 for $G = \mathrm{Spin}_7$, and type A_1, F_4, or E_6 for $G = E_6^{\mathrm{sc}}$. But $\alpha(\rho(\mathrm{Fr}_r))$, $\alpha \in \Delta$ are distinct, so $G_\rho = G(\bar{\mathbb{Q}}_l)$ in all three cases (see the proof of [Patrikis 2016, Lemma 7.8]). $\qquad\square$

Remark 4.19. As we have flexibilities in choosing $g \in G(\mathcal{O})$ lifting $\bar{\rho}(\mathrm{Fr}_r)$, it is easy to see that there are infinitely many lifts ρ that are nonconjugate in G^{ad}.

4B3. SL_2. The alternating group A_n admits a unique nontrivial central extension $\tilde{A}_n$ by $\mathbb{Z}/2\mathbb{Z}$ for $n \neq 6, 7$. By a result of N. Vila and J.-F. Mestre (which was proven independently, see [Serre 1992]), $\tilde{A}_n$ can be realized as a Galois group over $\mathbb{Q}$. In particular, we get a surjection $\bar{r} : \Gamma_{\mathbb{Q}} \twoheadrightarrow \tilde{A}_5$. On the other hand, $\tilde{A}_5$ can be described as follows: the symmetries of an icosahedron induce a 3-dimensional irreducible faithful representation of A_5, i.e., there is an injective homomorphism $A_5 \to \mathrm{SO}(3)$. The pullback of A_5 along the two-fold covering map $\mathrm{SU}(2) \twoheadrightarrow \mathrm{SO}(3)$ is a nontrivial central extension of A_5 by $\mathbb{Z}/2\mathbb{Z}$, hence is isomorphic to $\tilde{A}_5$. In particular, we get an embedding $\tilde{A}_5 \to \mathrm{SL}_2(\mathbb{C})$. As the matrix entries of the image lie in a finite extension of $\mathbb{Q}$, we can choose a finite extension k of $\mathbb{F}_l$ for which there is an embedding $\tilde{A}_5 \to \mathrm{SL}_2(k)$. Precomposing it with $\bar{r}$, we obtain a representation $\Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(k)$ which we denote by $\bar{\rho}$. It is easy to see that the adjoint module $\bar{\rho}(\mathfrak{sl}_2(k))$ is irreducible.

Let S be a finite set of places containing the archimedean place and all places where $\bar{\rho}$ is ramified. We impose no condition at l, and take the minimal prime to l deformation condition at all other places

in S, which is legitimate since the residual image has order prime to l for $l > 120$. Let $\Sigma \in \tilde{A}_5$ be an element of order 4, whose image in $\mathrm{SL}_2(k)$ is conjugate to $\mathrm{diag}(\sqrt{-1}, -\sqrt{-1})$. As $\tilde{A}_5$ has trivial abelian quotient, $\mathbb{Q}(\mu_l)$ and $\mathbb{Q}(\bar{\rho})$ are linearly disjoint over $\mathbb{Q}$. So there is an element $\sigma \in \Gamma_{\mathbb{Q}}$ such that $\bar{\rho}(\sigma) = \Sigma$ and $\bar{\kappa}(\sigma) = -1$. By Chebotarev's density theorem, there is a prime $p \notin S$ for which $\mathrm{Fr}_p = \sigma$. Therefore, $\bar{\rho}|_{\Gamma_p}$ is of Steinberg type and we take the Steinberg deformation condition at p.

Proposition 4.20. *For $\bar{\rho} : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(k)$ defined as above and for almost all primes l, there is an l-adic lift*

$$\rho : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(\mathcal{O})$$

of $\bar{\rho}$ with Zariski-dense image in $\mathrm{SL}_2(\overline{\mathbb{Q}}_l)$.

Proof. We first show that Theorem 3.4 applies to $\bar{\rho}$. Item (1) is satisfied: the left hand side of the inequality equals the right hand side. Item (2) is satisfied since $|\mathrm{Gal}(K/\mathbb{Q})|$ has order prime to l by the definition of $\bar{\rho}$. Item (3) is satisfied since $\bar{\rho}(\mathfrak{g})$ and $\bar{\rho}(\mathfrak{g})(1)$ are nonisomorphic. For item (4), we take σ to be as above, the connected component of whose centralizer is denoted T, and take α to be a root of $\Phi(G, T)$. So (a) is satisfied. As $\bar{\rho}(\mathfrak{g})$ is irreducible, (b) and (c) are satisfied.

Therefore, we can deform $\bar{\rho}$ to a continuous representation $\rho : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(\mathcal{O})$ satisfying the prescribed local conditions on S and the Ramakrishna condition on a set of auxiliary primes disjoint from S. We write G_ρ for the Zariski closure of the image of ρ in $\mathrm{SL}_2(\overline{\mathbb{Q}}_l)$. As $\bar{\rho}(\mathfrak{g})$ is irreducible, $\mathrm{Lie}(G_\rho)$ is either trivial or $\mathfrak{g}_{\overline{\mathbb{Q}}_l}$. If the former were true, then G_ρ would be finite. But $\rho|_{\Gamma_p}$ is Steinberg, so in particular the image of ρ is infinite, a contradiction. Thus $\mathrm{Lie}(G_\rho) = \mathfrak{g}_{\overline{\mathbb{Q}}_l}$. $\qquad\square$

Now we finish the proof of Theorem 1.2 with the congruence conditions removed. For G a simple but not simply connected group, suppose there is a homomorphism $\rho_l : \Gamma_{\mathbb{Q}} \to G^{\mathrm{sc}}(\overline{\mathbb{Q}}_l)$ with Zariski-dense image. We compose ρ_l with the covering projection $G^{\mathrm{sc}}(\overline{\mathbb{Q}}_l) \twoheadrightarrow G(\overline{\mathbb{Q}}_l)$, the resulting map has Zariski-dense image in $G(\overline{\mathbb{Q}}_l)$. Propositions 4.14, 4.18 and 4.20 prove the cases of a simple, simply connected classical group, E_6 and E_7. On the other hand, the remaining cases G_2, F_4, and E_8 have already been established in [Patrikis 2016] in a way similar to the proof of Proposition 4.18. So Theorem 1.2 is proved.

In order to remove the congruence conditions for G of type B_n, C_n and E_7, we impose the same local deformation conditions as specified in the paragraph preceding Lemma 4.11, but then use Theorem 3.21 instead of Theorem 3.16. By Lemmas 4.11 and 3.22, the assumptions in Theorem 3.21 are all met. Therefore, we obtain a characteristic zero lift of $\bar{\rho}$ satisfying the prescribed local conditions for *all* large enough primes l. Then the proof of Proposition 4.14 shows that the lift has full monodromy group for all large enough primes.

5. Connected reductive groups as monodromy groups

Following [Milne 2007], a connected algebraic group G is said to be an *almost-direct product* of its algebraic subgroups $G_1, \ldots, G_n$ if the map

$$G_1 \times \cdots \times G_n \to G : (g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$$

is a surjective homomorphism with finite kernel; in particular, this means that the G_i's commute with each other and each G_i is normal in G.

The following proposition is [Milne 2007, Corollary 4.4].

Proposition 5.1. *An algebraic group is semisimple if and only if it is an almost direct product of simple algebraic groups.* (*Here a simple algebraic group is called almost simple in [Milne 2007]*).

Proposition 5.2 (Goursat's lemma). *Let G_1, G_2 be groups, let H be a subgroup of $G_1 \times G_2$ such that the two projections $p_1 : H \to G_1$, $p_2 : H \to G_2$ are surjective. Let N_1 and N_2 be the kernels of p_2 and p_1, respectively. Then the image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \cong G_2/N_2$.*

Proposition 5.3. *Let G be a connected semisimple group, then there are continuous homomorphisms*

$$\Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$$

with Zariski-dense image for large enough l.

Proof. This will follow from Goursat's lemma, Theorem 1.2 and Remark 1.3. By Proposition 5.1, it suffices to prove the case when G is the direct product of simply connected simple algebraic groups. We may decompose G into "isotypic factors": $G = G_1 \times \cdots \times G_n$, where G_i is the direct product of copies of some simple algebraic group, and G_i, G_j have different types for $i \neq j$. Suppose we are given $\rho_i : \Gamma_{\mathbb{Q}} \to G_i(\bar{\mathbb{Q}}_l)$ with Zariski-dense image for each i and let $\rho := (\rho_1, \ldots, \rho_n) : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$, whose Zariski-closure is denoted by H. Then H is an algebraic subgroup of $G(\bar{\mathbb{Q}}_l)$ for which $\mathrm{pr}_i(H) = G_i(\bar{\mathbb{Q}}_l)$. Since $G_i(\bar{\mathbb{Q}}_l)$ and $G_j(\bar{\mathbb{Q}}_l)$ share no common nontrivial quotients for $i \neq j$, Proposition 5.2 implies that $H = G(\bar{\mathbb{Q}}_l)$.

It remains to prove the case when G is a direct product of copies of some simply connected simple algebraic group. Write $G = K^n$ with K simple. We first assume $K \neq \mathrm{SL}_2$. By Section 4B1 and 4B2 (especially Remarks 4.15 and 4.19), there exists a prime p and a homomorphism $\rho_i : \Gamma_{\mathbb{Q}} \to K(\bar{\mathbb{Q}}_l)$ for $1 \leq i \leq n$ such that ρ_i has Zariski-dense image and is unramified at p with $\rho_i(\mathrm{Fr}_p)$ a regular semisimple element in $K(\bar{\mathbb{Q}}_l)$, and for $i \neq j$, the images of $\rho_i(\mathrm{Fr}_p)$ and $\rho_j(\mathrm{Fr}_p)$ in $K^{\mathrm{ad}}(\bar{\mathbb{Q}}_l)$ are not conjugate by an automorphism of K^{ad}. Now we use Proposition 5.2 and induction on n to show that $\rho := \prod_i \rho_i : \Gamma_{\mathbb{Q}} \to G(\bar{\mathbb{Q}}_l)$ has Zariski-dense image. This is clear when $n = 1$. Suppose this is true for $n-1$, so that $\prod_{i < n} \rho_i : \Gamma_{\mathbb{Q}} \to K^{n-1}(\bar{\mathbb{Q}}_l)$ has Zariski-dense image. Let H be the Zariski-closure of the image of ρ and apply Proposition 5.2 to $p_1 : H \to G_1 = K^{n-1}$, $p_2 : H \to G_2 = K$, which are surjective by assumption, we see that the image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $G_1/N_1 \cong G_2/N_2$. But since $G_2 = K$ is a simple, simply connected algebraic group, $N_2 = K$ or $N_2 \subset Z(K)$. Also note that N_1 is either K^{n-1} or isogenous to the product of $n - 2$ factors in K^{n-1}. If $N_2 = K$ and $N_1 = K^{n-1}$, H must be G; otherwise, $N_2 \subset Z(K)$ and N_1 is isogenous to the product of $n - 2$ factors in K^{n-1}, so the isomorphism $G_1/N_1 \times G_2/N_2$ induces an isomorphism between two factors in $G^{\mathrm{ad}} = (K^{\mathrm{ad}})^n$. But this is impossible, as for any $i \neq j$, the images of $\rho_i(\mathrm{Fr}_p)$ and $\rho_j(\mathrm{Fr}_p)$ in $K^{\mathrm{ad}}(\bar{\mathbb{Q}}_l)$ are not conjugate by an automorphism of K^{ad}. Therefore, $H = G$.

Now let $K = \mathrm{SL}_2$. By the argument in the previous paragraph, it suffices to show that for any n, we can construct homomorphisms $\rho_i : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(\bar{\mathbb{Q}}_l)$, $1 \leq i \leq n$ such that ρ_i has Zariski-dense image and for

$i \neq j$, ρ_i^{ad} and ρ_j^{ad} are not conjugated by an automorphism of PGL_2. By the construction in [Serre 1992, 9.3] there are infinitely many homomorphisms $r : \Gamma_{\mathbb{Q}} \twoheadrightarrow \tilde{A}_5$ such that the composites $\Gamma_{\mathbb{Q}} \xrightarrow{r} \tilde{A}_5 \to A_5$ are ramified at different sets of finite primes. By Section 4B3 we then obtain infinitely many homomorphisms $\bar{\rho} : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(k)$ such that the corresponding homomorphisms $\bar{\rho}^{\mathrm{ad}} : \Gamma_{\mathbb{Q}} \to \mathrm{PGL}_2(k)$ are ramified at different sets of finite primes. By Proposition 4.20, we can deform $\bar{\rho}$ to characteristic zero with Zariski-dense image. We take n of them, denoted by $\rho_1, \ldots, \rho_n : \Gamma_{\mathbb{Q}} \to \mathrm{SL}_2(\overline{\mathbb{Q}}_l)$. Suppose for some i, j with $1 \leq i \neq j \leq n$, ρ_i^{ad} and ρ_j^{ad} were conjugate by an automorphism of PGL_2, then their mod l reductions $\bar{\rho}_i^{\mathrm{ad}}$ and $\bar{\rho}_j^{\mathrm{ad}}$ would be conjugate as well. But since there exists a prime p for which $\bar{\rho}_i^{\mathrm{ad}}$ is ramified at p and $\bar{\rho}_j^{\mathrm{ad}}$ is unramified at p, $\bar{\rho}_i^{\mathrm{ad}}$ and $\bar{\rho}_j^{\mathrm{ad}}$ cannot be conjugate, a contradiction. $\qquad\square$

Lemma 5.4. *Let n be a positive integer and $T = (\mathbb{G}_m)^n$. Then there is a continuous map $\iota : \mathbb{Z}_l \to T(\mathbb{Q}_l)$ with Zariski-dense image.*

Proof. The group T has only countably many connected proper Zariski-closed subgroups, so one can pick a line L in $\mathrm{Lie}(T)_{\mathbb{Q}_l}$ avoiding the tangent spaces to all such proper subgroups (since $\mathbb{Q}_l$ is uncountable). A small compact neighborhood of 0 in L exponentiates to a compact subgroup C of $T(\mathbb{Q}_l)$ whose Zariski closure has identity component that cannot be a proper algebraic subgroup of T, so C is Zariski-dense in T. $\qquad\square$

Now we can prove Theorem 1.1: Let G be a connected reductive group, then G is a quotient of the product of G^{der} (a semisimple group) and $Z(G)^0$ (a torus). Proposition 5.3 and Lemma 5.4 then allow us to build a homomorphism from $\Gamma_{\mathbb{Q}}$ to $G(\overline{\mathbb{Q}}_l)$ with Zariski-dense image for large enough l.

Acknowledgement

References

[Adams and He 2017] J. Adams and X. He, "Lifting of elements of Weyl groups", *J. Algebra* **485** (2017), 142–165. MR Zbl

[Bourbaki 1968] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres IV–VI*, Actualités Scientifiques et Industrielles **1337**, Hermann, Paris, 1968. Translated as *Lie groups and Lie algebras, chapters 4–6*, Springer, 2002. MR Zbl

[Buzzard and Gee 2014] K. Buzzard and T. Gee, "The conjectural connections between automorphic representations and Galois representations", pp. 135–187 in *Automorphic forms and Galois representations, I* (Durham, 2011), edited by F. Diamond et al., London Math. Soc. Lecture Note Ser. **414**, Cambridge Univ. Press, 2014. MR Zbl

[Clozel et al. 2008] L. Clozel, M. Harris, and R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l Galois representations", *Publ. Math. Inst. Hautes Études Sci.* **108** (2008), 1–181. MR Zbl

[Cornut and Ray 2018] C. Cornut and J. Ray, "Generators of the pro-p Iwahori and Galois representations", *Int. J. Number Theory* **14**:1 (2018), 37–53. MR Zbl

[Dettweiler and Reiter 2010] M. Dettweiler and S. Reiter, "Rigid local systems and motives of type G_2", *Compos. Math.* **146**:4 (2010), 929–963. MR Zbl

[Fakhruddin et al. 2018] N. Fakhruddin, C. Khare, and S. Patrikis, "Lifting irreducible Galois representations", preprint, 2018. arXiv

[Fontaine and Mazur 1995] J.-M. Fontaine and B. Mazur, "Geometric Galois representations", pp. 41–78 in *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), edited by J. Coates and S.-T. Yau, Ser. Number Theory **1**, Int. Press, Cambridge, MA, 1995. MR Zbl

[Fontaine and Messing 1987] J.-M. Fontaine and W. Messing, "p-adic periods and p-adic étale cohomology", pp. 179–207 in *Current trends in arithmetical algebraic geometry* (Arcata, CA, 1985), edited by K. A. Ribet, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, 1987. MR Zbl

[Gan and Yu 2003] W. T. Gan and J.-K. Yu, "Schémas en groupes et immeubles des groupes exceptionnels sur un corps local, I: Le groupe G_2", *Bull. Soc. Math. France* **131**:3 (2003), 307–358. MR Zbl

[Greenberg 2016] R. Greenberg, "Galois representations with open image", *Ann. Math. Qué.* **40**:1 (2016), 83–119. MR Zbl

[Humphreys 1995] J. E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Math. Surveys and Monographs **43**, Amer. Math. Sci., Providence, RI, 1995. MR Zbl

[Katz 2018] N. M. Katz, "A note on Galois representations with big image", preprint, 2018, Available at https://tinyurl.com/katzbig.

[Kostant 1959] B. Kostant, "The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group", *Amer. J. Math.* **81** (1959), 973–1032. MR Zbl

[Kret and Shin 2016] A. Kret and S. W. Shin, "Galois representations for general symplectic groups", preprint, 2016. arXiv

[LMFDB 2013] LMFDB Collaboration, "The L-functions and modular forms database", 2013, Available at http://www.lmfdb.org.

[Milne 2007] J. S. Milne, "Semisimple algebraic groups in characteristic zero", preprint, 2007. arXiv

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Math. Wissenschaften **323**, Springer, 2000. MR Zbl

[Patrikis 2016] S. Patrikis, "Deformations of Galois representations and exceptional monodromy", *Invent. Math.* **205**:2 (2016), 269–336. MR Zbl

[Ramakrishna 2002] R. Ramakrishna, "Deforming Galois representations and the conjectures of Serre and Fontaine–Mazur", *Ann. of Math.* (2) **156**:1 (2002), 115–154. MR Zbl

[Ribet 1985] K. A. Ribet, "On l-adic representations attached to modular forms, II", *Glasgow Math. J.* **27** (1985), 185–194. MR Zbl

[Saxl and Seitz 1997] J. Saxl and G. M. Seitz, "Subgroups of algebraic groups containing regular unipotent elements", *J. London Math. Soc.* (2) **55**:2 (1997), 370–386. MR Zbl

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Res. Notes in Math. **1**, Jones and Bartlett, Boston, MA, 1992. MR Zbl

[Serre 1996] J.-P. Serre, "Exemples de plongements des groupes $\mathrm{PSL}_2(\mathbb{F}_p)$ dans des groupes de Lie simples", *Invent. Math.* **124**:1-3 (1996), 525–562. MR Zbl

[Taylor 2003] R. Taylor, "On icosahedral Artin representations, II", *Amer. J. Math.* **125**:3 (2003), 549–566. MR Zbl

[Weston 2004] T. Weston, "Unobstructed modular deformation problems", *Amer. J. Math.* **126**:6 (2004), 1237–1252. MR Zbl

[Yun 2014] Z. Yun, "Motives with exceptional Galois groups and the inverse Galois problem", *Invent. Math.* **196**:2 (2014), 267–337. MR Zbl

tang@math.utah.edu   *Department of Mathematics, University of Utah, Salt Lake City, UT, United States*

Algebra & Number Theory

Algebra & Number Theory